Serge Gutwirth · Ronald Leenes
Paul de Hert · Yves Poullet *Editors*

European Data Protection: Coming of Age

Springer

European Data Protection: Coming of Age

Serge Gutwirth • Ronald Leenes • Paul de Hert
Yves Poullet
Editors

European Data Protection: Coming of Age

Springer

Editors
Serge Gutwirth
Faculty of law and criminology
Law, Science, Technology & Society (LSTS)
Vrije universiteit Brussel
Belgium

Paul de Hert
Faculty of law and criminology
Law, Science, Technology & Society (LSTS)
Vrije universiteit Brussel
Belgium

Ronald Leenes
TILT
Tilburg University
Tilburg, The Netherlands

Yves Poullet
Research Centre for Information
Technology & Law
University of Namur
Namur, Belgium

ISBN 978-94-007-5184-2 ISBN 978-94-007-5170-5 (eBook)
DOI 10.1007/978-94-007-5170-5
Springer Dordrecht Heidelberg New York London

Library of Congress Control Number: 2012953478

Printed on acid-free paper

Springer is part of Springer Science+Business Media (www.springer.com)

Foreword

The present book is one of the results of the 5th edition of the yearly Brussels based international conference *Computers, Privacy and Data Protection 2012 – CPDP2012*. Held on 25, 26 and 27 January 2012 under the title *European Data Protection: Coming of Age* the conference welcomed 692 participants at the venue, while another 500 people were reached through free public events organized in the evenings. The 3 day conference offered participants 25 panels and several workshops and special sessions, with 237 speakers from academia, the public and private sectors, and civil society.

Indeed, this year, the conference, which is traditionally organized around 28 January – 'Privacy day' – already had great momentum as it kicked off on the precise day (25 January 2012) that the European Commission presented its new 'Data protection package' consisting of a new 'Proposal for a Regulation on the protection of individuals with regards to the processing of personal data and on the free movement of such data' (the so-called General Data Protection Regulation) and a 'Proposal for a Directive on the protection of individuals with regards to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data'. These proposals for the amendment of the current EU data protection framework were not only impressive in volume – together they comprise of no less than 155 articles (and 172 pages) – but are also wide-reaching and ambitious in scope. The Regulation in particular is a detailed document, each provision of which invites discussion in terms of aim, effectiveness and proportionality. All participants will remember the packed *Grande Halle* in the late afternoon of Wednesday 25 January 2012: the attendees absolutely focused – so focused one could hear a pin drop – listening to the presentation of the Data Protection Package by Françoise Le Bail, EC Director General for Justice, and the first comments by highly qualified commentators. Many participants saw the effects of their scientific work, or stakeholder action, taking form (or not…) in the Commission's elaborated proposals. With a number of clearly new, or re-considered, directions put forward, this, undoubtedly was the starting shot for a probably long,

but still highly challenging, process of discussion, negotiation and lobbying, which will take place in the year 2012 and probably beyond.

European data protection: coming of age? has definitely been a good choice of title for CPDP2012. The Data Protection Package can indeed be described as a turning point, a rebirth of European data protection, and perhaps, its passage from an impulsive youth to a more mature state. The Commission tried to analyze, digest and 'reboot' data protection on the basis of almost 20 years of experience, stakeholders activity, scientific research and political decision making in the field. As such, this was no small achievement. However, the debate is open, and in the few months that followed, proposals had already been thoroughly commented and criticized, and amendments had already been proposed. Indeed, this encompassing renewal process of European data protection will be at the very heart of CPDP2013 which will take place on the 23, 24 and 25 January 2013 under the motto *Reloading data protection* (http://www.cpdpconferences.org/).

This book brings together chapters originating from two tracks. On the one hand, some chapters originate from responses to the conference's call for papers and have thus already been presented during the conference; on the other hand, some papers were submitted by invited speakers in the months following the conference. All the chapters of this book have been peer reviewed and commented on by at least two referees with expertise and interest in the subject matter. Since their work is crucial for maintaining the scientific quality of the book we would explicitly take the opportunity to thank them, *ad nominatim,* for their commitment and efforts: Antoinette Rouvroy, Anton Vedder, Cecile de Terwangne, Charles Raab, Caterine Flick, Claudia Diaz, Colin Bennett, Daniel Le Métayer, Daniel Lopez Gomez, Dara Hallinan, Ebeneser Paintsil, Eleni Kosta, Els De Busser, Eva Lievens, Gabriela Bodea, George Carlisle, Gerrit Hornung, Gloria González Fuster, Hans Hedbom, Ivan Szekely, Julien Jeandesboz, Joerg Daubert, Johann Cas, Joseph Savarimuthu, Karim Hadjri, Katja De Vries, Laura Tielemans, Lee Andrew Bygrave, Leonardo Martucci, Lothar Fritsch, Marc Langheinrich, Marc van Lieshout, Marit Hansen, Mathias Beckerle, Mathias Vermeulen, Michael Herrmann, Michel Arnaud, Mireille Hildebrandt, Pedro Bueso Guillen, Philip Schütz, Rachel Finn, Raphaël Gellert, Rob Heyman, Rocco Bellanova, Ronald Leenes, Ruddy Verbinnen, Seda Gürses, Serge Gutwirth, Simone Fischer-Hübner, Steve Paulussen, Tal Zarsky, and Wouter Steijn.

This volume brings together some 19 chapters, offering conceptual analyses, highlighting issues, proposing solutions, and discussing practices regarding privacy and data protection. In the first part of the book, conceptual analyses of concepts such as privacy and anonymity are provided. The second part focuses on the contrasted positions of digital natives and ageing users in the information society. The third part provides four chapters on privacy by design, including a contribution from the mother of privacy by design, Ontario Information and Privacy Commissioner Ann Cavoukian, as well as discussions on roadmapping and concrete techniques. The fourth part is devoted to a recurring CPDP theme, surveillance and profiling, with illustrations from the domain of smart metering, self-surveillance and the

benefits and risks of profiling. The book concludes with case studies pertaining to communicating privacy in organisations, the fate of a data protection supervisor in one of the EU member states, and data protection in social network sites and online media.

We hope this book will meet the reader's appetite!

Serge Gutwirth, Ronald Leenes, Paul De Hert, and Yves Poullet

Contents

Part I
Concepts

Chapter 1
Seven Types of Privacy

Rachel L. Finn, David Wright, and Michael Friedewald

1.1 Introduction

Theoretical and legal conversations about the relationship between technology and privacy date back to the 1890s with the advent of portable photography equipment accessible to the general population.[1] As technologies continue to develop, conceptualisations of privacy have developed alongside them, from a "right to be let alone" to attempts to capture the complexity of privacy issues within frameworks that highlight the legal, social-psychological, economic or political concerns that technologies present. However, this reactive highlighting of concerns or intrusions does not provide an adequate framework though which to understand the ways in which privacy should be proactively protected. Rights to privacy, such as those enshrined in the European Charter of Fundamental Rights, require a forward-looking privacy framework that positively outlines the parameters of privacy in order to prevent intrusions, infringements and problems. One such framework is presented by Roger Clarke, who, in the mid-1990s, identified four different categories of privacy, which

[1] Samuel Warren and Louis D. Brandeis, "The Right to Privacy," *Harvard Law Review* 4 (1890).

R.L. Finn (✉) • D. Wright
Crown House, Trilateral Research & Consulting, 72 Hammersmith Road,
London, W14 8TH, UK
e-mail: rachel.finn@trilateralresearch.com; david.wright@trilateralresearch.com

M. Friedewald
Fraunhofer Institute for Systems and Innovation Research ISI, Breslauer Straße 48,
76139 Karlsruhe, Germany
e-mail: michael.friedewald@isi.fraunhofer.de

S. Gutwirth et al. (eds.), *European Data Protection: Coming of Age*,
DOI 10.1007/978-94-007-5170-5_1,

enabled him to outline specific protections.[2] His four categories have been adopted by others, and appear in the privacy impact assessment handbooks of Australia and the United Kingdom.[3]

Clarke was the first privacy scholar of whom we are aware to have categorised the types of privacy in a logical, structured, coherent way. Others, such as Solove, have also developed a taxonomy of privacy.[4] However, Solove's taxonomy focuses on privacy harms rather than characterising the types of privacy.

Since Clarke's conceptualisation, new and emerging technologies have introduced further privacy effects, and Clarke's four categories are no longer sufficient to address the concerns they introduce. This paper makes a contribution to a forward-looking privacy framework by examining the privacy impacts of six new and emerging technologies. It analyses the privacy issues that each of these technologies present and argues that despite his initial capturing of the heterogeneity of privacy categories, Clarke's taxonomy must be revised and expanded to include seven different types of privacy. We also use this case study information to suggest that an imprecise conceptualisation of privacy may be necessary to maintain a fluidity that enables new dimensions of privacy to be identified, understood and addressed in order to effectively respond to rapid technological evolution.

1.2 Defining and Conceptualising Privacy

"Privacy" is a key lens though which many new technologies, and most especially new surveillance technologies, are critiqued.[5] However, "privacy" has proved notoriously difficult to define. Serge Gutwirth says "The notion of privacy remains out of the grasp of every academic chasing it. Even when it is cornered by such additional modifiers as 'our' privacy, it still finds a way to remain elusive."[6] Colin Bennett notes that "attempts to define the concept of 'privacy' have generally not met with any success".[7] Legal scholars James Whitman and Daniel Solove have

[2] Roger Clarke, "Introduction to Dataveillance and Information Privacy, and Definitions of Terms" (Xamax Consultancy, Aug 1997). http://www.rogerclarke.com/DV/Intro.html. Clarke identified these four categories even earlier, in his PhD Supplication in 1995. See http://www.rogerclarke.com/DV/PhD.html. He has variously referred to the four categories as categories, interests, dimensions, components and aspects. We use the term "types," which Gary T. Marx also uses. See Gary T. Marx, "Privacy is not quite like the weather" in *Privacy Impact Assessment*, edited by David Wright and Paul De Hert (Dordrecht: Springer, 2012).

[3] Office of the Privacy Commissioner, Privacy Impact Assessment Guide, Sydney, NSW, August 2006, revised May 2010, p. iii. Information Commissioner's Office (ICO), *Privacy Impact Assessment Handbook*, Wilmslow, Cheshire, UK, Version 2.0, June 2009, p. 14.

[4] See Daniel Solove, *Understanding Privacy* (Cambridge: Harvard University Press, 2008).

[5] David Lyon, *Surveillance after September 11* (Cambridge: Polity Press, 2003).

[6] Serge Gutwirth, *Privacy and the information age* (Lanham, MD: Rowman & Littlefield, 2002), 30.

[7] Colin J. Bennett, *Regulating Privacy: Data Protection and Public Policy in Europe and the United States* (Ithaca NY: Cornell University Press, 1992).

respectively described privacy as "an unusually slippery concept,"[8] and "a concept in disarray. Nobody can articulate what it means".[9] Furthermore, Debbie Kaspar notes that "scholars have a famously difficult time pinning down the meaning of such a widely used term [and] …most introduce their work by citing this difficulty".[10] Helen Nissenbaum has argued that privacy is best understood through a notion of "contextual integrity," where it is not the sharing of information that is a problem, rather it is the sharing of information outside of socially agreed contextual boundaries.[11] Political scientists have also discussed privacy in relation to state power, arguing that privacy has to be understood in connection with the other political rights that it allows individuals to exercise by protecting autonomy.[12] Others have focused on the economics of privacy, discussing how privacy is threaded through economic inequality, capitalism and private property. Christian Fuchs argues that in the economic context privacy is beneficial to companies and wealthy individuals because it masks income inequality, while privacy is simultaneously undermined by these very same companies who seek to control workers and consumers.[13] Feminist scholars have traced the ways in which appeals to privacy have been used to supported and reinforce gender inequality.[14] Still other scholars have pointed out that privacy has a social value as well and, indeed, is a bedrock of democracy itself.[15] Gutwirth explains why: privacy is "a cornerstone of contemporary Western society because it

[8] James Q. Whitman, "The Two Western Cultures of Privacy: Dignity Versus Liberty," *The Yale Law Journal* 113 (2004): 1153–54.

[9] Solove, 12. Solove believes that privacy is not one thing, that there is no common dominator. We can agree with that – in so far as we have identified seven types of privacy. However, we believe that there *is* a common denominator and that common denominator is the ill-defined notion of privacy itself. While we agree with Gutwirth, Priscilla Regan and others who say that privacy has a social value, privacy at its core relates to the integrity and autonomy of the individual, so that when privacy is compromised – no matter what type of privacy – the individual is being harmed in some way.

[10] Debbie V. S. Kaspar, "The Evolution (or Devolution) of Privacy," *Sociological Forum* 20 (2005): 72.

[11] Helen Nissenbaum, "Privacy as Contextual Integrity," *Washington Law Review,* 79:1 (2004), 101–139.

[12] Benjamin J. Goold, "Surveillance and the Political Value of Privacy," *Amsterdam Law Forum* 1 (2009): 5.

[13] Christian Fuchs, "Towards an alternative concept of privacy," *Journal of Information, Communication and Ethics in Society* 9 (2011): 232.

[14] Catharine A. MacKinnon, *Feminism Unmodified: Discourses on Life and Law* (Cambridge MA: Harvard University Press, 1987).

[15] The Supreme Court of Canada has stated that "society has come to realize that privacy is at the heart of liberty in a modern state." R. v. Dyment (188), 55 D.L.R. (4th) 503 at 513 (S.C.C.). On the social value of privacy, see, for example, Priscilla M. Regan, *Legislating Privacy: Technology, Social Values, and Public Policy, (*Chapel Hill, University of North Carolina Press, 1995), 220–231; Alan Westin, "Social and Political Dimensions of Privacy," *Journal of Social Issues*, 59: 2 (2003), 431–453; Valerie Steeves, "Reclaiming the social value of privacy," in Ian Kerr, Valerie Steeves and Carole Lucock (eds.), *Lessons from the Identity Trail: Anonymity, Privacy and Identity in a Networked Society* (Oxford University Press, 2009).

affects individual self-determination; the autonomy of relationships; behavioural independence; existential choices and the development of one's self; spiritual peace of mind and the ability to resist power and behavioural manipulation."[16]

Although a widely accepted definition of privacy remains elusive, there has been more consensus on a recognition that privacy comprises multiple dimensions, and some privacy theorists have attempted to create taxonomies of privacy problems, intrusions or categories. For example, Solove asserts that privacy is best understood as a "family of different yet related things".[17] Solove arrives at this conclusion by outlining a taxonomy of privacy problems that must be addressed, regardless of whether they conform to a precise definition of privacy. His taxonomy includes problems related to *information collection*, such as surveillance or interrogation, problems associated with *information processing*, including aggregation, data insecurity, potential identification, secondary use and exclusion, *information dissemination*, including exposure, disclosure breach of confidentiality, etc. and *invasion*, such as issues related to intrusion and decisional interference.[18] A typology of privacy intrusions is also offered by Debbie Kaspar, who argues that privacy cannot be understood unless examined from the inside. Kaspar distinguishes between invasions involving extraction, observation and intrusion.[19] *Extraction*-based privacy invasions involve making a deliberate effort to obtain something from a person. *Observation*-based privacy invasions are characterised by active and ongoing surveillance of a person, while *intrusion*-based invasions involve an "unwelcome presence or interference" in a person's life.[20]

However, these scholars' focus on the ways in which privacy can be infringed and the legal problem which must be solved is largely reactive. They focus on specific harms which are already occurring and which must be stopped, rather than over-arching protections that should be instituted to prevent harms. The difference between a taxonomy of privacy harms and a taxonomy of types of privacy is the pro-active, protective nature of the latter. It's the difference between outlawing murder and adopting a right to life. Murder is only one way in which life can be undermined, and a simple prohibition against murder would enable the dissolution of safety principles, etc. Instead, a positive right to life forces individuals, governments and other organisations to evaluate how their activities may impact upon a right to life and introduce protective measures.

Roger Clarke's approach to defining categories of privacy does assist in outlining what specific elements of privacy are important and must be protected. Clarke's four categories of privacy, outlined in 1997, include privacy of the person, privacy of

[16] Gutwirth, *Privacy and the information age*, 30.

[17] Solove, *Understanding Privacy*, 9.

[18] Daniel Solve, "'I've Got Nothing to Hide' and Other Misunderstandings of Privacy," *San Diego Law Review* 44 (2007): 758.

[19] Kaspar, *Evolution of Privacy*, 76.

[20] Ibid.

personal data, privacy of personal behaviour and privacy of personal communication.[21] *Privacy of the person* has also been referred to as "bodily privacy" and is specifically related to the integrity of a person's body. It would include protections against physical intrusions, including torture, medical treatment, the "compulsory provision of samples of body fluids and body tissue" and imperatives to submit to biometric measurement. For Clarke, privacy of the person is thread through many medical and surveillance technologies and practices. *Privacy of personal behaviour* includes a protection against the disclosure of sensitive personal matters such as religious practices, sexual practices or political activities. Clarke notes that there is a space element included within privacy of personal behaviour, where people have a right to private space to carry out particular activities, as well as a right to be free from systematic monitoring in public space. *Privacy of personal communication* refers to a restriction on monitoring telephone, e-mail and virtual communications as well as face-to-face communications through hidden microphones. Finally, *privacy of personal data* refers to data protection issues. Clarke adds that, with the close coupling that has occurred between computing and communications, particularly since the 1980s, the last two aspects have become closely linked, and are commonly referred to as "information privacy".

1.3 Seven Types of Privacy

Despite the utility of these four categories, recent technological advances have meant that they are no longer adequate to capture the range of potential privacy issues which must be addressed. Specifically, technologies such as whole body imaging scanners, RFID-enabled travel documents, unmanned aerial vehicles, second-generation DNA sequencing technologies, human enhancement technologies and second-generation biometrics raise additional privacy issues, which necessitate an expansion of Clarke's four categories. We will use these new and emerging technologies to argue for an expansion to seven different types of privacy, including privacy of the person, privacy of behaviour and action, privacy of personal communication, privacy of data and image, privacy of thoughts and feelings, privacy of location and space and privacy of association (including group privacy).[22] Although these seven types of privacy may have some overlaps, they are discussed individually because they provide a number of different lenses through which to view the effects of case study technologies. In this section, we briefly outline each of these seven types of privacy before linking them with relevant information from new and emerging technologies in the next section.

[21] Roger Clarke, "Introduction to Dataveillance and Information Privacy, and Definitions of Terms," Xamax Consultancy, Aug 1997. http://www.rogerclarke.com/DV/Intro.html.

[22] These seven types of privacy were first elaborated in an annex prepared for the PRESCIENT D1 report, available at http://www.prescient-project.eu/prescient/inhalte/download/PRESCIENT-D1---final.pdf.

Privacy of the person encompasses the right to keep body functions and body characteristics (such as genetic codes and biometrics) private. According to Mordini, the human body has a strong symbolic dimension as the result of the integration of the physical body and the mind and is "unavoidably invested with cultural values".[23] Privacy of the person is thought to be conducive to individual feelings of freedom and helps to support a healthy, well-adjusted democratic society. This aspect of privacy is shared with Clarke's categorisation.

We extend Clarke's notion of privacy of personal behaviour to *privacy of behaviour and action*. This concept includes sensitive issues such as sexual preferences and habits, political activities and religious practices. However, the notion of privacy of personal behaviour concerns activities that happen in public space, as well as private space, and Clarke makes a distinction between casual observation of behaviour by a few nearby people in a public space with the systematic recording and storage of information about those activities.[24] The ability to behave in public, semi-public or one's private space without having actions monitored or controlled by others contributes to "the development and exercise of autonomy and freedom in thought and action".[25]

Privacy of communication aims to avoid the interception of communications, including mail interception, the use of bugs, directional microphones, telephone or wireless communication interception or recording and access to e-mail messages. This right is recognised by many governments through requirements that wiretapping or other communication interception must be overseen by a judicial or other authority. This aspect of privacy benefits individuals and society because it enables and encourages a free discussion of a wide range of views and options, and enables growth in the communications sector.

We expand Clarke's category of privacy of personal data to include the capture of images as these are considered a type of personal data by the European Union as part of the 1995 Data Protection Directive as well as other sources. This *privacy of data and image* includes concerns about making sure that individuals' data is not automatically available to other individuals and organisations and that people can "exercise a substantial degree of control over that data and its use".[26] Such control over personal data builds self-confidence and enables individuals to feel empowered. Like privacy of thought and feelings, this aspect of privacy has social value in that it addresses the balance of power between the state and the person.

Our case studies reveal that new and emerging technologies carry the potential to impact on individuals' *privacy of thoughts and feelings*. People have a right not to

[23] Emilio Mordini, "Whole Body Imaging at airport checkpoints: the ethical and political context," in *Towards Responsible Research and Innovation in the Information and Communication Technologies and Security Technologies Fields*, ed. René von Schomberg (Luxembourg: Publications Office of the European Union, 2011).

[24] Clarke, "Introduction to Dataveillance".

[25] Helen Nissenbaum, *Privacy in Context: Technology, Policy and the Integrity of Social Life* (Stanford CA: Stanford University Press, 2010), 82.

[26] Clarke, "Introduction to Dataveillance".

share their thoughts or feelings or to have those thoughts or feeling revealed. Individuals should have the right to think whatever they like. Such creative freedom benefits society because it relates to the balance of power between the state and the individual.[27] This aspect of privacy may be coming under threat as a direct result of new and emerging technologies.[28] Privacy of thought and feelings can be distinguished from privacy of the person, in the same way that the mind can be distinguished from the body. Similarly, we can (and do) distinguish between thought, feelings and behaviour. Thought does not automatically translate into behaviour. Similarly, one can behave thoughtlessly (as many people often do).

According to our conception of *privacy of location and space*, individuals have the right to move about in public or semi-public space without being identified, tracked or monitored. This conception of privacy also includes a right to solitude and a right to privacy in spaces such as the home, the car or the office. Such a conception of privacy has social value. When citizens are free to move about public space without fear of identification, monitoring or tracking, they experience a sense of living in a democracy and experiencing freedom. Both these subjective feelings contribute to a healthy, well-adjusted democracy. Furthermore, they encourage dissent and freedom of assembly, both of which are essential to a healthy democracy. This categorisation of privacy was also not as obviously under threat when Clarke was writing in 1997, however, this has changed with technological advances.

The final type of privacy that we identify, *privacy of association (including group privacy)*, is concerned with people's right to associate with whomever they wish, without being monitored. This has long been recognised as desirable (necessary) for a democratic society as it fosters freedom of speech, including political speech, freedom of worship and other forms of association. Society benefits from this type of privacy in that a wide variety of interest groups will be fostered, which may help to ensure that marginalised voices, some of whom will press for more political or economic change, are heard. This aspect of privacy was not considered by Clarke, and a number of new technologies outlined below could negatively impact upon individuals' privacy of association.

One might question what the difference is between privacy of location and space and privacy of behaviour. Privacy of location means that a person is entitled to move through physical space, to travel where she wants without being tracked and monitored. Privacy of behaviour means the person has a right to behave as she wants (to sleep in class, to wear funny clothes) so long as the behaviour does not harm someone else. Privacy of behaviour does not necessarily have anything to do with a person travelling through space, driving to work, going shopping or whatever. One can behave as one wants in private, separately from others. Privacy of association differs from privacy of behaviour because it is not only about groups or organisations (e.g., political parties, trade unions, religious groups, etc.) to which we choose to

[27] Goold, "Surveillance and the Political Value of Privacy".

[28] Dara Hallinan, Philip Schütz, and Michael Friedewald, "Neurodata-Based Devices and Data Protection" (paper presented at the 5th Bi-annual Surveillance and Society Conference, Sheffield, April 3–4, 2012).

belong, privacy of association also relates to groupings or profiles over which we have no control – for example, DNA testing can reveal that we are members of a particular ethnic group or a particular family. Privacy of association directly relates to other fundamental rights such as freedom of religion, freedom of assembly, etc., from which privacy of behaviour and action (as we define it) are a step removed.

Our typology of privacy (or, rather, our expansion of Clarke's typology) offers various benefits to a range of stakeholders. It is important above all in policy terms, i.e., policy-makers should ensure that these different types of privacy are adequately protected in legislation, i.e., it is not sufficient to protect only personal data and personal communications (e.g., against interception). This typology is also of instrumental value in the development of a privacy impact assessment methodology in Europe (as is being done in the EC-funded PIAF,[29] PRESCIENT[30] and SAPIENT[31] projects, for example). Similarly, organisations that carry out privacy impact assessments should be concerned not only about privacy of personal data and privacy of communications, but also the other types of privacy as well. We also believe our typology provides academics and other privacy experts with a useful, logical, well-structured and coherent typology in which to frame their privacy studies. Our typology is similarly useful for privacy advocates. Although a widely accepted definition of privacy has proven elusive, this typology, firmly building on that established by Clarke, should be widely accepted.

1.4 Privacy Impacts of New and Emerging Technologies

In this section, we discuss six new and emerging technologies and their potential impact upon the seven different types of privacy outlined above. We use whole body imaging scanners, RFID-enabled travel documents, unmanned aircraft systems (drones), second-generation DNA sequencing, human enhancement technologies and second-generation biometrics to illustrate the need to expand Clarke's four categories. For each technology, we examine what types of privacy they could infringe upon. We demonstrate that different technologies impact upon different types of privacy and that technological developments can introduce new and unforeseen facets of privacy. We also analyse these several new and emerging technologies in terms of their impact on one or more different types of privacy in order to assist policy-makers in understanding these new additional types of privacy and in devising protections that address all of these different types.

[29] www.piafproject.eu.

[30] www.prescient-project.eu.

[31] www.sapientproject.eu.

1.4.1 Whole Body Imaging Scanners

Whole body imaging scanners seek to address the fact that current technologies and screenings, such as walk-through metal detectors and hand searches, have deficiencies in detecting some types of threats, and that law enforcement and security staff need tools to enable them to deal with threats from explosives and non-metallic weapons.[32] Whole body imaging scanners, or body scanners, provide one possible means of reducing the threat from non-metallic weapons. Body scanners "produce an image of the body of a person showing whether or not objects are hidden in or under his clothes" by using x-ray backscatter or millimetre waves.[33] Given the sensitive nature of the images produced by body scanners, critics have raised privacy concerns in relation to their mass deployment, particularly at large airports, including the revealing of individuals' naked bodies and medical conditions and the protection of individuals' data and images. These concerns largely align with Clarke's understanding of bodily privacy, privacy of behaviour and action and privacy of personal data. However, these scanners generate images that we regard as part of personal data.

Bodily privacy concerns raised by body scanners have mainly centred on two key issues, the revealing of individuals' naked bodies and revealing information about medical conditions. In terms of revealing naked bodies, privacy advocates argue that this loss of privacy is disproportionate to any gains in security. Academics, privacy advocates, politicians and journalists have all warned that the images resulting from the different types of body scanners currently deployed in airports and other contexts reveal an individual's "naked body," including "the form, shape and size of genitals, buttocks and female breasts".[34] The issue of "naked images" has also raised questions surrounding child protection laws, and the Electronic Privacy Information Center (EPIC) has argued that the capacity for viewing, storage and recall of images of children may contravene child protection laws.[35] According to privacy advocates, the images also show details of medical conditions that may be embarrassing for individuals. In 2002, the American Civil Liberties Union (ACLU) asserted that "passengers expect privacy underneath their clothing and should not be required to display highly personal details of their bodies…as a pre-requisite to boarding a plane".[36] Despite these concerns, authorities, such as the UK Department for

[32] Silvia Venier, "Global Mobility and Security," *Biometric Technology Today* 5 (2009).

[33] European Commission, Consultation: The impact of the use of body scanners in the field of aviation security on human rights, privacy, personal dignity, health and data protection, Brussels, 19 February 2009.

[34] Demetrius Klitou, "Backscatter body scanners – A strip search by other means," *Computer Law & Security Report* 24 (2008): 317.

[35] Electronic Privacy Information Center, "Transportation Agency's Plan to X-Ray Travelers Should Be Stripped of Funding," last modified June 2005, http://epic.org/privacy/surveillance/spotlight/0605/.

[36] American Civil Liberties Union, "The ACLU's view on body scanners," last modified 15 March 2002, http://www.aclu.org/technology-and-liberty/body-scanners.

Transport, have argued that any loss of body privacy is proportionate and legitimate in relation to the security concerns that body scanners address.[37]

Images generated from body scanners could also reveal information about behaviour such as augmentation surgeries or medical related practices. For example, the ACLU has argued that body scanners reveal medical or lifestyle behaviour such as evidence of mastectomies, colostomy appliances, penile implants and/or catheter tubes, and thus provide details about individual behaviour. In terms of body imaging scanners, the issues related to privacy of behaviour and action significantly overlap with bodily privacy, however, the two are separate in the sense that it is the activities revealed by the images which individuals wish to conceal rather than the bodies or images themselves.

Concerns around data protection and data privacy revolve around protection of personal data that the scanners generate, including the storage and transmission of images. According to the US Transportation Safety Administration (TSA) the scanners used in US airports do not store, print or transmit images.[38] However, a Freedom of Information Act request by EPIC to the TSA found that machines come with the capability to store and transmit images, but this is disabled when they are deployed to airports.[39] EPIC argues that the fact that this capability could be re-enabled represents a data protection risk to passengers.[40] EPIC further notes that the TSA does not have a stellar reputation for protecting passenger data.[41] Privacy International is also concerned that some employees operating scanners will experience an "irresistible pull" to store or transmit images if a "celebrity or someone with an unusual… body goes through the system".[42] In fact, images from body imaging scanners have been posted on the Internet in a breach of the fundamental rights of thousands of people in the USA.[43] However, despite the link between body imaging scanners and privacy

[37] Department for Transport, *Impact Assessment on the use of security scanners at UK airports*, last modified 29 March 2001. http://webarchive.nationalarchives.gov.uk/+/http://www.dft.gov.uk/consultations/open/2010-23/.

[38] Ki Mae Heussner, "Air Security: Could Technology Have Stopped Christmas Attack?," *ABC News*, 29 December 2009. http://abcnews.go.com/Technology/AheadoftheCurve/air-security-technology-stopped-xmas-attack/story?id=9436877.

[39] Kim Zetter, "Airport Scanners Can Store, Transmit Images," *Wired News*, 11 January 2010. http://www.wired.com/threatlevel/2010/01/airport-scanners/.

[40] Philip Rucker, "US airports say seeing is believing as passengers face body-scan drill," *Sydney Morning Herald,* 5 January 2010. http://www.smh.com.au/travel/travel-news/us-airports-say-seeing-is-believing-as-passengers-face-bodyscan-drill-20100104-lq6o.html.

[41] EPIC, "Transportation Agency's Plan to X-Ray Travelers Should Be Stripped of Funding".

[42] Privacy International, "PI statement on proposed deployments of body scanners in airports," last modified 31 December 2009. https://www.privacyinternational.org/article/pi-statement-proposed-deployments-body-scanners-airports.

[43] European Economic and Social Committee, Opinion of the European Economic and Social Committee on the Communication from the Commission to the European Parliament and the Council on the Use of Security Scanners at EU airports, COM(2010) 311 final, Brussels, 16 February 2011, 4.

of personal data, the body scanners example makes clear that Clarke's conception of personal data needs to be expanded to include images as personal data.[44] Thus, data protection laws control the unauthorised storage, transfer and disclosure of personal data, precisely the issues of concerns that are expressed in relation to the images produced by body imaging scanners.

1.4.2 RFID-Enabled Travel Documents

RFID-enabled travel documents include travel cards, such as Oyster Cards in London, which integrate RFID technology with the use of mass transportation in urban areas and RFID-enabled passports, also called e-passports, which are currently being introduced in most countries. Such RFID-enabled travel documents raise privacy concerns within the categories of privacy of behaviour and action, privacy of data and image and privacy of location and space.

Privacy of behaviour and action can be negatively impacted by RFID-enabled travel documents, in that people's behaviours and travel activities can be reconstructed or inferred from information generated as a result of their use of these technologies. Travel routes, frequent destinations and mode of transport can be gleaned from information available on both e-passport databases and travel card databases. Location, time and other information stored on databases can be combined, which police have used to check the whereabouts or movements of suspects' during criminal investigations.[45] Furthermore, aggregated information can provide details that enable travellers' routines to be inferred. This can also materialise into a mistaken identity threat in that the association between an individual and a tag can be spurious (e.g., if the travel card or passport is stolen or given to another person), but the initial association is difficult to break once it is made.[46]

The relative (in)security of personal information on databases represents a threat to personal data protection. RFID systems are composed of tags, readers and back-end databases. In RFID-enabled travel cards, the unique identifier on the chip is linked with personal information (e.g., if a person pays for the card by credit card, London Underground will have a record of all his or her travels and travel times). In RFID-enabled passports, the personal information stored on the chip can also be

[44] Even if the images are anonymised, this would not legitimate the circulation of such images. Circulation of such images without the authorisation of the person whose image was captured would be either illegal or morally repugnant or both.

[45] *The Guardian*, "Oyster data use rises in crime clampdown," 13 March 2006. http://www.guardian.co.uk/technology/2006/mar/13/news.freedomofinformation and Octopus Holdings Limited, "Customer Data Protection".

[46] Marc Langheinrich, "A survey of RFID privacy approaches," *Personal and Ubiquitous Computing* 13 (2009): 414.

compromised by being read directly and without authorisation from the chip. Unauthorised reading may take place in public space, can occur without the passport holder's knowledge, and can violate data protection principles in that it can be used to reveal an individual's personal details, biometric information and/or their citizenship. Although basic protection measures such as access codes and Faraday cages[47] are built into e-passports to prevent unauthorised reading, Gellert and Gutwirth argue that these measures do not provide adequate protection[48] and do not possess the desired long-term security needed for e-passport applications (their validity is estimated to a maximum of 10 years).[49] Systems that store personal data, including biometric data, in back-end databases may also be vulnerable to data protection threats such as hacking, unauthorised access or unauthorised disclosure. Some systems have attempted to protect individuals from this threat by separating personal information from the RFID chip in the e-passport.[50] However, the resulting databases which store the sensitive personal information could represent a vulnerability. Finally, the unauthorised *use* of personal information also represents a privacy threat. In terms of RFID-enabled travel cards, marketing staff can target individuals based on the personal data they are required to submit in an application form and companies could aggregate these pieces of information to construct sophisticated consumer profiles.[51] This is especially true if contactless travel cards are expanded for use as payment for other small items.

Privacy of location and space is another aspect of privacy that is potentially undermined by RFID-enabled travel documents. Both RFID-enabled travel cards and e-passports carry the potential for a location threat, whereby individuals' movements can be monitored based on the RFID signature of their documents. Langheinrich argues that once a tag is associated with a particular person, the presence of the tag implies a location disclosure.[52] Information about where an individual has been can also be accessed after the fact using information on databases that store information about when and where documents have been read. While this information could be useful for the individual concerned in terms of billing or payment disputes, it may also harm individuals whose location information is revealed to third parties. Travellers may also be vulnerable to hotlisting, which consists of

[47] Faraday cages are a metallic shielding embedded in the passport cover and designed to protect it from electronic eavesdropping.

[48] Faraday cages do not prevent eavesdropping on legitimate conversations between readers and tags, and basic access codes could enable counterfeiting, since a forger could splice together a valid electronic signature with false identity information and biometric components.

[49] Raphael Gellert and Serge Gutwirth, "Privacy, data protection and policy issues in RFID enabled e-passports," in *Privacy, data protection and ethical issues in new and emerging technologies: Five case studies*, eds. Rachel Finn and David Wright (PRESCIENT consortium, 25 November 2011).

[50] Marc van Lieshout, et al., *RFID Technologies: Emerging Issues, Challenges and Policy Options*, Office for Official Publications of the European Communities, Luxembourg, 2007, 197.

[51] Lara Srivastava, "Radio frequency identification: ubiquity for humanity," *info* 9 (2007).

[52] Langheinrich, "RFID privacy approaches".

compiling all the available information concerning an individual, so that when an identifier is detected it can be linked to all the other information available concerning this particular individual.[53] In consequence, authorities could be informed that a travel document connected to a particular individual, or an individual with particular characteristics, has been read in a particular place at a particular time. This generalised threat materialises into specific threats, such as stalking[54] or unauthorised location disclosures to spouses, or other individuals.[55] However, in most places, police or other authorities must obtain a search warrant or court order in order to be given access to the data.[56] Finally, the RFID signals in passports or travel cards may also be tracked, since most RFID tags are standardised and will broadcast their signal to any compatible reader. This means that an individual could read an RFID chip's unique identifier, store it and follow its signal as long as the RFID reader is within range of the RFID-embedded travel card.

1.4.3 Unmanned Aircraft Systems

Despite a slow increase in the introduction of UASs in civil applications, such as law enforcement, border patrol and other regulatory surveillance, the use of unmanned aircraft systems (UASs or drones) has generated relatively muted debate about privacy and data protection. Privacy is notable by its absence in many discussions about UAS devices, which may be partly explained by their current similarity to existing forms of surveillance such as CCTV surveillance or surveillance by police helicopter. However, the lack of noise and relative invisibility of UASs mean that individuals do not know if they are being monitored and UAS surveillance may often occur covertly.[57] Our discussion demonstrates that UASs raise issues of privacy of behaviour and action, privacy of data and image, privacy of location and space and privacy of association.

With surveillance-oriented drones, everyone is monitored regardless of whether their activities warrant suspicion; therefore, all behaviours are monitored and recorded. This potential for negative impacts on privacy of behaviour and action is

[53] A. Juels, D. Molnar and D. Wagner, "Security and Privacy Issues in E-passports," in *Proceedings of IEEE/Create-net SecureComm 2005*, (Los Angeles CA: IEEE Computer Society Press, 2005), 79.

[54] Organisation for Economic Co-operation and Development, "RFID Guidance and Reports," *OECD Digital Economy Papers* 152 (Paris: OECD publishing, 2008), 42.

[55] Steve Bloomfield, "How an Oyster Card can Ruin your Marriage," *The Independent on Sunday*, 19 February 2006. http://www.independent.co.uk/news/uk/home-news/how-an-oyster-card-could-ruin-your-marriage-467077.html.

[56] Octopus Holdings Limited, "Customer Data Protection," 2009.

[57] Rachel L. Finn and David Wright, "Unmanned aircraft systems: Surveillance, ethics and privacy in civil applications," *Computer Law & Security Review* 28:2 (2012).

particularly significant since UAS surveillance is much less overt than CCTV or helicopter surveillance to which it has been compared. The potential to use surveillance covertly means that in order to protect themselves from the negative effects of intrusions, individuals must assume they are being surveilled at all times and attempt to adjust their behaviour accordingly. This could introduce anticipatory conformity (a "chilling effect") where individuals alter their behaviour because they believe they may be under surveillance.[58]

UAS surveillance potentially infringes upon privacy of data and image in that it can generate images of individuals, sometimes covertly. This means that data protection principles contained in the 1995 Data Protection Directive (as well as the proposed Data Protection Regulation[59]) such as transparency, consent and rights of access can be undermined, because individuals may not even realise that they are subject to UAS surveillance at any given moment. Therefore, potentially covert data capture also leaves individuals with a limited ability to exercise privacy by taking "measures to keep private those activities that they do not wish to expose to public view".[60] One particular group who could be disproportionately affected by deployments of UASs in civil air space are celebrities whom paparazzi or other media could target with drones.

UAS devices can infringe upon privacy of location and space in that they can be used to track people or undermine their expectations regarding the boundaries of personal space. These surveillance devices can capture images of a person or a vehicle in public space, thereby placing individuals in particular places at particular times or revealing their movements through public space if more than one image is captured. UASs may also reveal information about private spaces such as back yards or, when flying low, can even transmit images of activities captured within homes, offices or other apparently private spaces. Thus, individuals who assume that their activities are not being monitored because they occur within the home or within private property may find that this assumption is false. The fact that this surveillance can be covert makes the capture of this information particularly problematic.

UAS devices may impact upon privacy of association through their ability to monitor individuals and crowds, again, sometimes covertly. Unmanned aircraft systems can generate information about groups or individuals with whom they associate. For example, at protests or other large gatherings of people, the number and organisation of individuals can be analysed, and group membership can be inferred. If UAS visual surveillance was combined with biometrics such as facial recognition technology, individual group membership and affiliation could be discovered. Furthermore, group activities can also be identified or analysed, for example, place and time of meetings and activities at meetings.

---

[58] Paul McBride, "Beyond Orwell: The Application of Unmanned Aircraft Systems in Domestic Surveillance Operations," *Journal of Air Law and Commerce* 74 (2009): 659.

[59] European Commission, Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), COM(2012) 11 final, Brussels, 25 January 2012.

[60] McBride, "Beyond Orwell," 661.

1.4.4 Second-Generation DNA Sequencing Technologies

Second-generation DNA sequencing technologies refer to the routine sequencing of the whole genomes of individuals rather than just distinct parts of the genome. Second-generation DNA sequencing impacts on the privacy of the person through the collection of intimate information that can potentially reveal personal data that are classified as sensitive. DNA sequences can reveal sensitive information about an individual and may indicate specific human qualities such as sex, sexual orientation, ethnicity, physical and mental health and predispositions to certain behaviours.[61] These categories are often associated with social marginalisation and discrimination, and revealing these traits can have significant impacts in terms of privacy of data and image. If this data is routinely revealed, individuals could become vulnerable to the consequences of genetic testing or could be effectively forced to undergo genetic testing in order to obtain insurance, employment or access to other goods and services.[62] These consequences could affect the individuals as well as their family members, due to the heritability of genetic information. As a result, second-generation DNA sequencing can impact upon privacy of the person, privacy of data and image, privacy of location and space and privacy of association.

Second-generation DNA sequencing impacts on the privacy of the person through the collection of intimate information that can potentially reveal personal data that are classified as sensitive. Currently, some police forces, such as those in the UK, are able to use reasonable force to take a DNA sample from arrested individuals, and military personnel in the USA are only able to refuse to submit a DNA sample for serious religious reasons.[63] While in these cases the taking of DNA samples does not take place on the basis of a mutual consent, this may change in the near future. Setting up biobanks for biomedical research involves the recruitment of large population cohorts and whole genome DNA sequencing will likely become a routine diagnostic test method in some areas of health care (e.g., for prenatal diagnosis). These examples suggest that consent could gradually become undermined as mandatory volunteerism becomes more commonplace.[64]

Second-generation DNA sequencing technologies potentially infringe upon the privacy of a person's data or image. As highlighted above, the information generated by DNA sequencing can potentially reveal sensitive data that increases the

[61] *Nature Biotechnology*, "DNA confidential," Editorial, 27 (2009): 777.

[62] Piret Kukk, Bärbel Hüsing and Michael Friedewald, "Privacy, data protection and policy issues in next generation DNA sequencing technologies," *Privacy, data protection and ethical issues in new and emerging technologies: Five case studies*, eds. Rachel Finn and David Wright (PRESCIENT consortium, 25 November 2011).

[63] Dorothy Nelkin and Lori Andrews, "DNA identification and surveillance creep," *Sociology of Health & Illness* 21 (1999).

[64] Gary T. Marx, "Soft Surveillance: The Growth of Mandatory Volunteerism in Collecting Personal Information – 'Hey Buddy Can You Spare a DNA?'," in *Surveillance and Security: Technological Politics and Power in Everyday Life*, ed. T. Monahan (London: Routledge, 2006).

potential for genetic discrimination by government, insurers, employers, schools, banks and others.[65] Furthermore, despite the assumption that genetic data in databases can be rendered anonymous, it is possible that individuals could be identified,[66] with all of the associated consequences. Lunshof et al. identify several avenues through which individuals could be de-anonymised, including:

- Inferring phenotype from genotype by identifying information in DNA and RNA, for instance, stature, hair or iris colour, or skin colour, or ethnic group
- Any amount of DNA data in the public domain with a name allows for identification within any anonymised data set
- Security breaches based on attacks on or thefts or loss of DNA data.[67]

As such, like many other emerging technologies, the link between individuals and a "data set" requires a significant amount of attention to data protection mechanisms in order to protect privacy.

Whole genome DNA sequencing can negatively impact on privacy of location and space. This is primarily centred on concerns over the potential for detecting someone's location by comparing the DNA sample found at a specific location and people's DNA profiles. This can be grounds for making associations between persons and their location, especially within forensics. It also introduces a possibility for making spurious associations between individuals and particular locations as a result of secondary transfers as this technology becomes more sensitive. Although whole genome sequencing is an emerging technology still in the research domain, the recent advent of low copy number DNA techniques[68] have led to mistakes in the criminal justice system, including false positive matches that suggested an individual's presence in a particular location[69] and matches resulting from secondary transfers associated with contamination.[70]

Finally, second-generation whole genome sequencing potentially impacts upon privacy of association in negative ways. An individual's presence at a particular gathering could be detected through linking a person's DNA profile with DNA found at that location. Individuals could be categorised into particular groups based on information gleaned from their DNA sequence, and profiling enables individuals within particular groups to be identified. Furthermore, in addition to identification, but in a similar frame, whole genome DNA sequencing could allow the use of DNA

[65] Kukk et al., "Next-generation DNA sequencing".

[66] L. Curren, et al., "Identifiability, genomics and UK data protection law," *European Journal of Health Law* 17 (2010).

[67] J.E. Lunshof et al., "From genetic privacy to open consent," *Nature Reviews Genetics* 9 (2008).

[68] Wikipedia defines Low Copy Number (LCN) as a DNA profiling technique developed by the Forensic Science Service (FSS) and in use in some countries since 1999.

[69] Rebecca Fowler, "Coded Revelations: DNA the second revolution," *The Observer*, 27 April 2003.

[70] Alan Hall, "Woman serial killer was a just phantom, German police admit," *The Telegraph*, 26 March 2009. http://www.telegraph.co.uk/news/worldnews/europe/germany/5056339/Woman-serial-killer-was-a-just-phantom-German-police-admit.html.

of one family member to provide information about another. For example, whole genome sequencing could identify when people are related and reveal information about whether another family member has committed a crime or if they are likely to be carriers for particular diseases, etc.[71]

1.4.5 Human Enhancement

Human enhancement technologies include those which offer enhancement via pharmacological means, i.e., neuro-enhancing pharmaceuticals (neuro-enhancers), or technical means via brain-computer interfaces (BCIs).[72] Neuro-enhancing pharmaceuticals are characterised by their biological and chemical effects, and pharmaceutical neuro-enhancement comprises not only illegal drugs (amphetamines or cocaine), but also over-the-counter drugs such as aspirin and prescription drugs such as antidepressants and methylphenidate (Ritalin). However, prescription drugs such as Ritalin may be misused or intentionally used for other purposes than the prescribed ones. The two most important categorisations of BCIs, particularly in relation to their privacy invasiveness, is their location (invasive vs. non-invasive) and whether they operate from human to machine and/or vice versa. Although machine-to-human operation can be found in medical applications such as deep brain stimulation, most BCI technology operates from human to machine and is used to enable the user to control other digital or mechanical devices without the actual need of any neuro-muscular movement. Electroencephalography (EEG) that measures the electrical impulses emitted by the brain is the most prevalent sensing technology, and applications such as the mental typewriter or brain-to-robot interfaces are currently primarily being developed for therapeutic purposes. However, such technology could become more prevalent since the gaming and entertainment industry has recently shown an interest in the "reading" of brain activity to control and manipulate applications.[73] These human enhancement technologies carry the potential to impact upon privacy of the person, privacy of behaviour and action, privacy of communication, privacy of data and image and privacy of thoughts and feelings.

Human enhancement may violate privacy of the person, both through neuro-enhancing pharmaceuticals and brain-computer interfaces, when the method of

[71] Dustin Hays and DNA Policy Centre, "DNA, Forensics, and the Law," last modified 2008. http://www.dnapolicy.org/policy.issue.php?action=detail&issuebrief_id=42.

[72] Philip Schütz and Michael Friedewald, "Technologies for Human Enhancement and their impact on privacy," in *Privacy, data protection and ethical issues in new and emerging technologies: Five case studies*, eds. Rachel Finn and David Wright (PRESCIENT consortium, 25 November 2011).

[73] Anton Nijholt, "BCI for Games: A 'State of the Art' Survey," in *Entertainment Computing – ICEC 2008*, eds. Scott M. Stevens and Shirley J. Saldamarco (Berlin: Springer, 2009), 225.

enhancement implies the internalisation of substances or technologies and/or a potential loss of control. On the one hand, Schütz and Friedewald argue that pharmaceutical neuro-enhancers enable the prescribing authority to exercise control over the recipient, affecting his/her bodily privacy.[74] On the other hand, BCI technology is based on both human and machine learning processes, which means that it could be possible to manipulate the BCI user.[75] Thus, Schütz and Friedewald further argue that any gain in control through the use of BCIs could easily be offset by a potential for loss of control. This confronts the user with unintended and potentially devastating consequences, particularly if the individual is dependent on the BCI-linked technology. For example, Parkinson's patients using BCIs such as deep brain stimulation have been confronted with side effects that include a change in their personality.

Human enhancement technologies potentially impact upon privacy of behaviour and action in two ways. First, as mentioned above, neuro-enhancers are closely linked to the risk of losing control over one's will and actions. That is why prescribed "enhancing" drugs such as Ritalin or Modafinil pose a threat of external control over the individual's behaviour. Second, drawing on BCI technology, behavioural neuroscience allows the location of parts of the brain that are supposed to be responsible for certain kinds of behaviour, attitudes and actions. In this context, individuals could be exposed to preventive strategies, such as crime prevention.[76] Furthermore, individuals could be influenced to buy certain products, or spend more money than they otherwise would, based on an interaction between mood, purchasing behaviour and external stimulation.[77]

Privacy of communication may be impacted by brain-computer interfaces, whereby the interception or monitoring of data streams between the BCI user and the machine could be possible. When BCIs are used to assist individuals in communicating with others, the data that passes between the user and the communication software could be intercepted and analysed. Furthermore, recent scientific research in brain imaging and speech has begun to identify electrical patterns associated with certain words or phrases.[78] As BCIs develop, more of the content of communication could become vulnerable to interception.

Privacy of data and image is only touched upon in relation to human enhancement technologies that are capable of collecting data, regardless of how it may be further processed. As such, BCIs are the only human enhancement technology that

---

[74] Schütz and Friedewald, "Technologies for Human Enhancement and their impact on privacy".

[75] Dennis J. McFarland and Jonathan R. Wolpaw, "Brain-computer interfaces for communication and control," *Communications of the ACM* 54 (2011): 63.

[76] Adam Kepecs, "Neuroscience: My brain made me do it," *Nature* 473 (2011).

[77] Ira van Keulen and Mirjam Schuijff, "Engineering of The Brain: Neuromodulation and Regulation," in *Making Perfect Life: Bioengineering in the 21st Century*, eds. Rinie van Est and Dirk Stemerding (Brussels: European Technology Assessment Group, June 2011).

[78] Ian Sample, "Mind-reading program translates brain activity into words," *The Guardian*, 31 January 2012. http://www.guardian.co.uk/science/2012/jan/31/mind-reading-program-brain-words.

potentially impacts upon privacy of data and image because they involve the digitalisation, collection, (temporary) storage and processing of information about brain activity. This data is highly sensitive, because the prospective worth of such unique personal information may increase exponentially in terms of its marketing value for the advertisement industry. In addition, it is difficult to anticipate what information can be collected and/or extracted in the future and whether it will be financially lucrative. Despite this, Schütz and Friedewald note that system security was given little thought when researchers first developed the technical infrastructure of BCIs, as was the case in the early days of the Internet. Thus, BCI technologies are vulnerable to breaches through hacking or other intrusions.[79] However, at the moment, this threat is relatively inconsequential as current BCIs are not designed to extract data, they merely link individuals with other assistive technologies.

Furthermore, information from brain computer interfaces may be able to recognise and identify patterns that shed light on certain thoughts and feelings of the carrier. According to McFarland and Wolpaw, the images created by the brain's electrical impulses reveal an enormous depth of information about the individual, his/her mind and way of thinking. "For the first time it may be possible to breach the privacy of the human mind, and judge people not only by their actions, but also by their thoughts and predilections."[80] Such technologies are being explored in relation to counter-terrorism and advertising practices, where, for example, sensor networks are being deployed in semi-public spaces to detect stress levels to attempt to identify suspicious behaviour and are being developed for retail situations to attempt to predict and influence purchasing behaviour. In the counter-terrorism context, such data could lead to additional questioning or refusal of services, which would impact upon a person's privacy of thoughts or feelings. Shoppers could also be influenced in the retail sector or targeted based on the feelings that they present, leading to discrimination or other profiling practices. In either context, such technology could encourage individuals to attempt to conceal thoughts or feelings in anticipation of such measurements since their thoughts or feelings could become public information.

1.4.6 Second-Generation Biometrics

In parallel with their wider deployment, biometrics have raised critical privacy and data protection issues which have impacted the acceptability of biometric identification methods. The next generation of biometrics include the measurement

[79] Medical Device Security Center, "Medical Device Security Center," last modified 2011. http://secure-medicine.org/.

[80] Martha J. Farah, "Neuroethics: The practical and the philosophical," *Trends in Cognitive Sciences* 9 (2005): 34.

and analysis of new biometric traits, such as behavioural or soft biometrics (i.e., biometrics which may change over time, such as gait analysis and voice recognition software) and physiological biometrics (including heartbeat detection, pheromone detection). In second-generation biometrics, these soft or physiological traits are often used in combination with more traditional traits in *multiple biometrics* or *multimodal systems* to strengthen identification systems. Venier and Mordini argue that the most critical implications of next-generation biometrics are that future biometric recognition could take place remotely, covertly and/or from a distance and may produce material with a high degree of sensitive (and surplus) information.[81] However, many of the applications of second-generation biometrics are still in the research domain and second-generation biometrics are most appropriately classed as emerging technologies. Unique to other technologies discussed here, second-generation biometrics affect all of the seven types of privacy we outline in this article. Some soft biometrics such as the way one walks (gait) or types a letter could be regarded as unconscious behaviour. However, we would regard these as still different from privacy of behaviour and action as these possibly supposed unconscious behaviours reflect a personal characteristic (privacy of the body) rather than the intentionality that is implicit in privacy of behaviour and action.

In relation to second-generation biometrics, privacy of the person could be impacted by the systematic collection of information that could be used for classification purposes. Venier and Mordini argue that second-generation biometrics potentially infringe upon human dignity through the measurement and digitalisation of the body.[82] Second-generation biometrics also involve the collection of intimate information, which carries the potential to reveal personal data that are classified as sensitive, including medical data, gender, age and/or ethnicity. Because of the potential for classification, Venier and Mordini are concerned that the *categorisation* of individuals could become a more sensitive issue than *identification* in terms of biometrics, as second-generation biometrics may enable subjects to be characterised via biometric profiling or be used to provide a link to an existing non-biometric profile.[83] This could be exacerbated as more, sometimes superfluous, data is collected by multiple biometrics and multimodal systems, in order to improve system performance. Furthermore, the collection of biometric information remotely, covertly and/or at a distance could mean that individuals' bodies are routinely measured and mined for information without the explicit consent of the person who is being monitored.

Soft biometrics potentially impact privacy of behaviour and action through processes of automation. According to Venier and Mordini, human behaviour can be monitored, captured, stored and analysed in order to enable systems to become

[81] Silvia Venier and Emilio Mordini, "Second-generation biometrics," in *Privacy, data protection and ethical issues in new and emerging technologies: Five case studies*, eds. Rachel Finn and David Wright (PRESCIENT consortium, 25 November 2011).

[82] Venier and Mordini, "Second-generation biometrics".

[83] Ibid.

knowledgeable about people. Subsequently, measurements of changes in behaviour and definitions of "abnormal" behaviour can also become automated which could lead to monitoring and recording of infrequent behaviours that are not suspicious or criminally deviant. Physiological biometrics may also impact privacy of behaviour and action by revealing sensitive information about a person's psychological state, which can be used for behaviour prediction, as a result of pre-emptive discriminatory measures.

Soft biometrics, specifically voice or speech recognition technologies, can negatively impact individuals' privacy of personal communications. Speech or voice recognition technologies can be utilised to record, analyse and disclose the content of communication. Although these are not the primary purpose of such technologies, the infrastructure necessary to record and verify human voices or human speech can be relatively easily re-worked to enable such recording and disclosure of the content of speech. Such re-oriented voice or speech recognition technologies can also be linked with automated systems to ensure that communications by certain individuals, or communications about certain topics, can be monitored or recorded. This could discourage individuals who use certain types of voice recognition systems from communicating with particular people or about particular topics in areas where voice recognition systems are in operation.

Soft biometrics and the use of biometrics at a distance both pose a threat to personal data and image. Article 33 of the proposed new Data Protection Regulation says that the processing of biometric data presents specific risks, meaning that it must be processed in respect of principles such as consent and proportionality. Some types of soft biometrics, and especially biometrics at a distance, can present a risk that an individual would not know that a system was in operation and thus would not have consented to the collection of their biometric information and may not be able to exercise their rights to access that data. Behavioural biometrics also introduce concerns over the storage of raw data (a person's image or video from cameras monitoring public areas) in databases and how this personal data is used given these new capabilities. Finally, the fact that soft biometrics often collect additional, unnecessary information raises issues surrounding the principle of proportionality.

Physiological biometrics can impact privacy of thoughts and feelings through the collection of intimate information that can be used to detect suspicious behaviour or predict intention or susceptibility. Imaging scanners that combine physiological measurements intended to detect heightened emotional states could provide clues to an individual's state of mind and potentially lead to discrimination.[84] This introduces a concern that human feelings become technically defined and represented and that automated decisions over and about individuals may be made based upon this information. Examples of such applications include counter-terrorism applications as well as personalised advertising applications where individuals' experience

[84] *Harvard Magazine*, "Where Decisionmaking is Measured," 12 December 2008. http://harvardmagazine.com/breaking-news/where-decisionmaking-is-measured.

of semi-public space is restricted or impacted by the emotional state "read" by biometric sensors. Again, the danger is not necessarily that the individual is identified, but that they are categorised and decisions are made about them based on the profile they present.

Second-generation biometrics such as embedded systems and soft biometrics may also negatively impact privacy of location and space. Unlike current-generation overt biometric systems used to authenticate or identify an individual with their co-operation, sensing and identifying individuals at a distance can result in covert data capture without the data subject's consent. This means that a biometric system can create a link between an individual and a location at a particular time without their co-operation, and without their being aware that this occurred. Thus, there is a clear overlap with the privacy concerns associated with privacy of the person. Individuals could also be tracked without being identified by using biometrics to differentiate a particular person as they move through public space. Here, biometrics can be used in tandem with other surveillance systems, such as CCTV, static cameras or mobile phones with location detection capabilities, to pinpoint or track an individual's location.

Finally, soft biometrics may negatively impact privacy of association. Soft biometrics introduces concerns that individual members of a group could be identified at a distance through the linking of such biometrics to other data sets. Furthermore, behavioural analysis could be used to identify leaders or vulnerable members of a group, enabling group organisation and decision-making structures to be revealed.

1.4.7 Filling in the Gaps

Despite the utility of Clarke's four categories of privacy, particularly in relation to the identification of specific types of privacy which must be protected, our case studies reveal that new and emerging technologies introduce new and additional types of privacy that Clarke did not consider in his original piece. Our conceptualisation maintains two of Clarke's original categories: privacy of the person and privacy of personal communication.[85] We have also re-worked Clarke's categories of privacy of personal behaviour and privacy of personal data to privacy of behaviour and action and privacy of data and image respectively. The change to privacy of behaviour *and action* is because we regard behaviour and action as both characterised by intentionality, but "action" is slightly different from "behaviour". Action has an element of planning that is not normally present in behaviour. We would not want to overstate this, however. One can act (behave) in a certain way in response to a certain stimulus (if someone slaps you in the face, you might slap back, and there probably is precious little time to "plan" such a response), but on the other hand, if

[85] As mentioned early on in this article, Clarke labelled privacy of personal data and privacy of personal communications as "information privacy".

you are an assassin, you probably have a fair amount of time to plan your next hit (action). The change to privacy of data and image is intended to highlight the image as a form of personal data that increasingly can be mined for biometric data and used to identify, monitor and/or track individuals as they move about public or semi-public space.

Furthermore, three additional aspects of privacy were necessary to fully capture the privacy impacts of the new and emerging technologies that we discussed here. Clarke's original framework did not include privacy of location and space, privacy of thoughts and feelings and privacy of association (including group privacy). Although Clarke includes some consideration of "space" within his category of privacy of behaviour, our understanding of location and space includes the potential to connect an individual to a particular location at a particular time, rather than simply monitoring that person as they move about in particular spaces. Furthermore, privacy of location and space includes the possibility that the individual moving about space can be connected to a digital persona, or that location information could be aggregated to actively or retrospectively track an identifiable individual as they move around in public or semi-public space (e.g., shopping malls) or private property (e.g., stores, office buildings). In addition to RFID-enabled travel documents, and the other examples discussed in this paper, automatic number plate recognition (ANPR) systems, CCTV cameras fitted with facial recognition and global positioning system surveillance such as chips carried in smart phones also perform similar functions with similar associated potential privacy impacts.

The inclusion of privacy of thoughts and feelings addresses another gap in Clarke's categorisation. Emerging technologies such as brain computer interfaces, as well as neuro-imaging, neural modulation and biometric sensor arrays (heart rate monitors, skin temperature sensors, pupil dilation) all have the possibility to disrupt the interiority of the body and mind to provide clues about thoughts, feelings and/or states of mind. This differs from privacy of the person in that privacy of the person focuses on identifying, reflecting and classifying the physical body, whereas privacy of thoughts and feelings targets the more ephemeral aspects of the person. Furthermore, privacy of thoughts and feelings protects what is perhaps the least controversial, most consistent and unwavering dimension of privacy, the individual thoughts and feelings which until now were almost entirely imperceptible to others unless individuals chose to share them.

Finally, privacy of association connects privacy, as a heterogeneous but largely individualised concept, to interpersonal relationships. As recognised by Article 8 of the Charter of Fundamental Rights, privacy includes respect for both individual and family life, thus inter-personal relationships form part of the European conception of privacy. Second, privacy of association links directly with other fundamental rights such as rights to assembly, religious freedom and free speech. New and emerging technologies enable individuals and their inter-relationships to be revealed through DNA sequencing technology that identifies family relationships or enables individuals to be organised into groups based on physical traits, technologies such as UAS surveillance or second-generation biometrics which can link identifiable individuals to particular places at particular times and behavioural analytic technologies

which can analyse behaviour to better understand relationships between group members and/or group structures. These additional aspects of privacy are most visible in relation to new and emerging technologies and have expanded our understanding of different types of privacy. The next section will examine how the heterogeneity and flexibility of privacy, as a concept, needs to be maintained in order to continue to address the potential impacts associated with technological developments.

1.5 The Merit of Elusiveness

As mentioned above, Gutwirth refers to a definition of privacy as "elusive". In this summary section, we argue that privacy is an inherently heterogeneous, fluid and multidimensional concept, and we suggest that this multidimensionality may be necessary to provide a platform from which the effects of new technologies can be evaluated. This potential necessity is supported by the fact that different technologies impact upon different types of privacy, and further technological changes may introduce or foreground previously unconsidered privacy dimensions.

Our case study discussion above demonstrates that different technologies potentially impact upon different types of privacy and embody different risks to privacy. Table 1.1, below, summarises the spread of privacy types that new and emerging technologies may impact upon. Consolidating the case study information illustrates that privacy of data and image and privacy of behaviour and action are threatened by most if not all new and emerging surveillance technologies. In contrast, privacy of thought and feelings and privacy of communication are potentially impacted by second-generation biometrics and human enhancement technology only. Therefore, scholars, legal theorists, policy-makers and other actors must maintain an awareness that there are different types of privacy in order to ensure adequate protection of individuals (and society) in relation to existing and emerging technologies, applications and practices.[86]

This also means that the protection of data that *describes* a person will remain important in the future. However, with the advent of new technologies such as next-generation biometrics, DNA sequencing and human enhancement technologies the data being collected moves from simply describing a person to being an *inherent part* of the person. This calls for a much stronger focus on an ethical assessment element to complement established (and enhanced) data protection principles.

[86] We do not mean to suggest that the newer the technology, the broader the risks to these different dimensions of privacy. Each new technology must be assessed to determine whether it has impacts on privacy and, if so, which types of privacy. It does not follow that new technologies necessarily pose greater risks to privacy than older technologies, but it is certainly true, as we have demonstrated, that some new technologies have exposed types of privacy not heretofore considered and that as technologies become more complex, the more likely it is that the risks will also be more complex.

Table 1.1 Aspects of privacy potentially impacted by case study technologies

	Technology					
Type of privacy	Whole body imaging scanners	RFID-enabled travel documents	Unmanned aircraft systems	Second-generation DNA sequencing	Human enhancement technologies	Second-generation biometrics
Privacy of the person	X			X	X	X
Privacy of behaviour and action	X	X	X	X	X	X
Privacy of communication					X	X
Privacy of data and image	X	X	X	X	X	X
Privacy of thought and feelings					X	X
Privacy of location and space		X	X	X		X
Privacy of association			X	X		X

We also suggest that the fluidity of privacy as a concept may be an important aspect of its utility, since technological developments may introduce new types of privacy. As technologies develop and proliferate, various types of privacy which had not previously been considered or identified as under threat may become compromised. While the privacy experts quoted in Sect. 1.2 lament the fact that privacy is difficult to define and conceptualise, we propose that fluidity and flexibility are necessary to enable "privacy" to respond to technological changes. More precise conceptualisations, taxonomies and boundaries surrounding privacy, particularly in the legal field, may disrupt the use of privacy to protect individuals and groups from intrusions that impact upon their freedoms, fundamental rights and access to goods and services.[87] Therefore, despite other theorists' frustration with the difficulty in defining privacy, perhaps maintaining its elusiveness carries particular benefits for law-makers and citizens. In any event, we believe that our typology offers benefits, as we stated earlier, for policy-makers, academics, privacy advocates and any organisation carrying out a reasonably comprehensive privacy impact assessment.

1.6 Conclusion

This paper has provided three main theoretical arguments. First, we have demonstrated that privacy is a fluid and dynamic concept that has developed alongside technological and social changes. In the 15 years between 1997 and 2012, the advent of new technologies and applications has meant that previously unconsidered types of privacy now need to be addressed in order to adequately protect individuals' rights, freedoms and access to goods and services. Second, we have identified seven different types of privacy that current decision-makers need to consider in providing proactive protection to individuals in the face of new and emerging technologies. These include privacy of the person, privacy of behaviour and action, privacy of data and image, privacy of communication, privacy of thoughts and feelings, privacy of location and space, and privacy of association (including group privacy). Each of the different technologies discussed here impact upon different types of privacy and all of these types need to be considered when formulating privacy protections.[88]

[87] We draw support in this conclusion from Gutwirth, *Privacy and the information age,* pp. 33–34, who discusses the undesirability of defining privacy from a legal perspective.

[88] Privacy should not be narrowly defined, nor should information privacy (of communication and personal data protection) be regarded as all there is to privacy. Clarke speaks of a "serious debasement of the term 'privacy' [which] has occurred in the case of U.S. and Australian statutes that have equated it with the highly restrictive idea of 'data protection'. That notion derives from the 'fair information practices' movement that has been used by corporations and governments since the late 1960s to avoid meaningful regulation." Roger Clarke, "What's 'privacy'?," Xamax Consultancy, 2006. http://www.rogerclarke.com/DV/Privacy.html.

Third, we have proposed that one of the strengths of privacy is its complexity, fluidity and heterogeneity. Decision-makers, and most especially policy-makers, may find benefit in maintaining a fluid and mutable understanding of privacy in order to ensure that privacy is protected in the face of future technological developments.

Acknowledgement This paper is based in part on research undertaken in the PRESCIENT (Privacy and Emerging Sciences and Technologies) project funded under the European Commission's 7th Framework Programme for research and technological development (SIS-CT-2009-244779). We thank Silvia Venier (CSSC), Piret Kukk and Philip Schütz (Fraunhofer ISI) for their important contributions to our research.

References

American Civil Liberties Union. The ACLU's view on body scanners. http://www.aclu.org/technology-and-liberty/body-scanners. Last modified 15 Mar 2002.

Bennett, Colin J. 1992. *Regulating privacy: Data protection and public policy in Europe and the United States*. Ithaca: Cornell University Press.

Bloomfield, Steve. 2006. How an oyster card can ruin your marriage. *The Independent on Sunday*, 19 Feb 2006. http://www.independent.co.uk/news/uk/home-news/how-an-oyster-card-could-ruin-your-marriage-467077.html.

Clarke, Roger. 2006. What's 'Privacy'?. *Australian Law Reform Commission Workshop*. http://www.rogerclarke.com/DV/Privacy.html. 28 July 2006.

Clarke, Roger. Aug 1997. Introduction to dataveillance and information privacy, and definitions of terms. Canberra: Xamax Consultancy. http://www.rogerclarke.com/DV/Intro.html.

Curren, L., P. Boddington, H. Gowans, N. Hawkins, N. Kanellopoulou, J. Kaye, and K. Melham. 2010. Identifiability, genomics and UK data protection law. *European Journal of Health Law* 17: 329–344.

Department for Transport. 2001. Impact assessment on the use of security scanners at UK airports. http://webarchive.nationalarchives.gov.uk/+/http://www.dft.gov.uk/consultations/open/2010-23/. 29 Mar 2001.

Electronic Privacy Information Center (EPIC). Transportation agency's plan to X-ray travelers should be stripped of funding. Last modified June 2005. http://epic.org/privacy/surveillance/spotlight/0605.

European Commission. Consultation: The impact of the use of body scanners in the field of aviation security on human rights, privacy, personal dignity, health and data protection. Brussels, 19 Feb 2009. http://ec.europa.eu/transport/air/consultations/2009_02_19_body_scanners_en.htm.

European Commission, Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), COM(2012) 11 final, Brussels, 25 January 2012.

European Economic and Social Committee. 2010. Opinion of the European Economic and Social Committee on the Communication from the Commission to the European Parliament and the Council on the Use of Security Scanners at EU airports. COM 311 final, Brussels, 16 Feb 2011.

Farah, Martha J. 2005. Neuroethics: The practical and the philosophical. *Trends in Cognitive Sciences* 9: 34–40.

Finn, Rachel L., and David Wright. 2012. Unmanned aircraft systems: Surveillance, ethics and privacy in civil applications. *Computer Law & Security Review* 28(2): 184–194.

Fowler, Rebecca. 2003. Coded revelations: DNA the second revolution. *The Observer*, 27 Apr 2003.

Fuchs, Christian. 2011. Towards an alternative concept of privacy. *Journal of Information, Communication and Ethics in Society* 9: 220–237.

Gellert Raphael, and Serge Gutwirth. 2011. Privacy, data protection and policy issues in RFID enabled e-passports. In *Privacy, data protection and ethical issues in new and emerging technologies: Five case studies* PRESCIENT Deliverable 2, ed. Rachel Finn and David Wright, 31–59. Report prepared by the PRESCIENT consortium for the European Commission's Directorate-General Research, 25 Nov 2011.

Goold, Benjamin J. 2009. Surveillance and the political value of privacy. *Amsterdam Law Forum* 1: 3–6.

The Guardian, Oyster data use rises in crime clampdown. 13 Mar 2006. http://www.guardian.co.uk/technology/2006/mar/13/news.freedomofinformation.

Gutwirth, Serge. 2002. *Privacy and the information age*. Lanham: Rowman & Littlefield.

Hall, Alan. 2009. Woman serial killer was just a phantom: German police admit. *The Telegraph*, 26 Mar 2009. http://www.telegraph.co.uk/news/worldnews/europe/germany/5056339/Woman-serial-killer-was-a-just-phantom-German-police-admit.html.

Hallinan, Dara, Philip Schütz, and Michael Friedewald, *"Neurodata-Based Devices and Data Protection"*. Paper presented at the 5th Bi-annual Surveillance and Society Conference, Sheffield, 3–4 April 2012

Harvard Magazine, Where decisionmaking is measured. 12 Dec 2008. http://harvardmagazine.com/breaking-news/where-decisionmaking-is-measured.

Hays, Dustin, and DNA Policy Centre. 2007. *DNA, Forensics, and the Law*. Last modified 2008. http://www.dnapolicy.org/policy.issue.php?action=detail&issuebrief_id=42.

Heussner, Ki Mae. 2009. Air security: Could technology have stopped Christmas attack? *ABC News*, 29 Dec 2009. http://abcnews.go.com/Technology/AheadoftheCurve/air-security-technology-stopped-xmas-attack/story?id=9436877.

Information Commissioner's Office (ICO), Privacy Impact Assessment Handbook, Wilmslow, Cheshire, UK, Version 2.0, June 2009

Juels, A., D. Molnar, and D. Wagner. 2005. Security and privacy issues in E-passports. In *Proceedings of IEEE/Create-net SecureComm 2005*, 74–88. Los Angeles: IEEE Computer Society Press.

Kaspar, Debbie V.S. 2005. The evolution (or devolution) of privacy. *Sociological Forum* 20: 69–92.

Kepecs, Adam. 2011. Neuroscience: My brain made me do it. *Nature* 473: 280–281. Accessed 2 Mar 2012. http://www.nature.com/doifinder/10.1038/473280a.

Klitou, Demetrius. 2008. Backscatter body scanners – A strip search by other means. *Computer Law & Security Report* 24: 316–325.

Kukk, Piret, Bärbel Hüsing and Michael Friedewald. 2011. Privacy, data protection and policy issues in next generation DNA sequencing technologies. In *Privacy, data protection and ethical issues in new and emerging technologies: Five case studies* PRESCIENT Deliverable 2, ed. Rachel Finn and David Wright, 143–174. Report prepared by the PRESCIENT consortium for the European Commission's Directorate-General Research, 25 Nov 2011.

Langheinrich, Marc. 2009. A survey of RFID privacy approaches. *Personal and Ubiquitous Computing* 13: 413–421.

Lunshof, J.E., R. Chadwick, D.B. Vorhaus, and G.M. Church. 2008. From genetic privacy to open consent. *Nature Reviews Genetics* 9: 406–411.

Lyon, David. 2003. *Surveillance after September 11*. Cambridge: Polity Press.

MacKinnon, Catharine A. 1987. *Feminism unmodified: Discourses on life and law*. Cambridge, MA: Harvard University Press.

Marx, Gary T. 2006. Soft surveillance: The growth of mandatory volunteerism in collecting personal information – 'Hey buddy can you spare a DNA?'. In *Surveillance and security: Technological politics and power in everyday life*, ed. Torin Monahan, 37–56. London: Routledge.

Marx, Gary T. 2012. Privacy is not quite like the weather. In *Privacy impact assessment*, ed. David Wright and Paul De Hert. Dordrecht: Springer.
McBride, Paul. 2009. Beyond Orwell: The application of unmanned aircraft systems in domestic surveillance operations. *Journal of Air Law and Commerce* 74: 627–662.
McFarland, Dennis J., and Jonathan R. Wolpaw. 2011. Brain-computer interfaces for communication and control. *Communications of the ACM* 54: 60–66.
Medical Device Security Center. 2011. *Medical Device Security Center*. http://secure-medicine.org/.
Mordini, Emilio. 2011. Whole body imaging at airport checkpoints: The ethical and political context. In *Towards responsible research and innovation in the information and communication technologies and security technologies fields*, ed. René von Schomberg, 165–209. Luxembourg: Publications Office of the European Union.
Nature Biotechnology. 2009. DNA confidential. Editorial 27: 777.
Nelkin, Dorothy, and Lori Andrews. 1999. DNA identification and surveillance creep. *Sociology of Health & Illness* 21: 689–706.
Nijholt, Anton. 2009. BCI for games: A 'State of the Art' survey. In *Entertainment computing – ICEC 2008*, ed. Scott M. Stevens and Shirley J. Saldamarco, 225–228. Berlin: Springer.
Nissenbaum, Helen. 2004. Privacy as contextual integrity. *Washington Law Review* 79(1): 101–139.
Nissenbaum, Helen. 2010. *Privacy in context: Technology, policy and the integrity of social life*. Stanford: Stanford University Press.
Octopus Holdings Limited. *Customer Data Protection*. Last updated 2009.
Office of the Privacy Commissioner, *Privacy Impact Assessment Guide*, Sydney, NSW, August 2006, revised May 2010
Organisation for Economic Co-operation and Development. 2008. RFID guidance and reports. *OECD Digital Economy Papers*, 152. Paris: OECD Publishing.
Privacy International. 2009. PI statement on proposed deployments of body scanners in airports. Last updated 31 Dec 2009. https://www.privacyinternational.org/article/pi-statement-proposed-deployments-body-scanners-airports.
Regan, Priscilla M. 1995. *Legislating privacy: Technology, social values, and public policy*, Chapel Hill: University of North Carolina Press.
Rucker, Philip. 2010. US airports say seeing is believing as passengers face body-scan drill. *Sydney Morning Herald*, 5 Jan 2010. http://www.smh.com.au/travel/travel-news/us-airports-say-seeing-is-believing-as-passengers-face-bodyscan-drill-20100104-lq6o.html.
Sample, Ian. 2012. Mind-reading program translates brain activity into words. *The Guardian*, 31 Jan 2012. http://www.guardian.co.uk/science/2012/jan/31/mind-reading-program-brain-words.
Schütz, Philip, and Michael Friedewald. 2011. Technologies for human enhancement and their impact on privacy. In *Privacy, data protection and ethical issues in new and emerging technologies: Five case studies* PRESCIENT Deliverable 2, ed. Rachel Finn and David Wright, 175–198. Report prepared by the PRESCIENT consortium for the European Commission's Directorate-General Research, 25 Nov 2011.
Solove, Daniel J. 2008. *Understanding privacy*. Cambridge, MA: Harvard University Press.
Solve, Daniel. 2007. 'I've got nothing to hide' and other misunderstandings of privacy. *San Diego Law Review* 44: 745–772.
Srivastava, Lara. 2007. Radio frequency identification: Ubiquity for humanity. *Info* 9: 4–14.
Steeves, Valerie. 2009. Reclaiming the social value of privacy. In *Lessons from the identity trail: Anonymity, privacy and identity in a networked society*, ed. Ian Kerr, Valerie Steeves, and Carole Lucock. Oxford: Oxford University Press.
Supreme Court of Canada, R. v. Dyment (188), 55 D.L.R. (4th) 503 at 513 (S.C.C.).
van Keulen, Ira, and Mirjam Schuijff. 2011. Engineering of the brain: Neuromodulation and regulation. In *Making perfect life: Bioengineering in the 21st century*, ed. Rinie van Est and Dirk Stemerding, 68–116. European Technology Assessment Group, June 2011.
van Lieshout, Marc, Luigi Grossi, Graziella Spinelli, Sandra Helmus, Linda Kool, Leo Pennings, Roel Stap, Thijs Veugen, Bram van der Waaij, and Claudio Borean. 2007. *RFID technologies:*

Emerging issues, challenges and policy options. Luxembourg: Office for Official Publications of the European Communities.
Venier, Silvia. 2010. Global mobility and security. *Biometric Technology Today* 5: 7–10.
Venier, Silvia and Emilio Mordini. 2011. Second-generation biometrics. In *Privacy, data protection and ethical issues in new and emerging technologies: Five case studies* PRESCIENT Deliverable 2, ed. Rachel Finn and David Wright, 111–142. Report prepared by the PRESCIENT consortium for the European Commission's Directorate-General Research, 25 Nov 2011.
Warren, Samuel, and Louis D. Brandeis. 1890. The right to privacy. *Harvard Law Review* 4: 193–220.
Westin, Alan. 2003. Social and political dimensions of privacy. *Journal of Social Issues* 59(2): 431–453.
Whitman, James Q. 2004. The two western cultures of privacy: Dignity versus liberty. *The Yale Law Journal* 113: 1151–1221.
Zetter, Kim. 2010. Airport scanners can store, transmit images. *Wired News*, 11 Jan 2010. http://www.wired.com/threatlevel/2010/01/airport-scanners/.

Chapter 2
The Internet as Surveilled Workplayplace and Factory

Christian Fuchs and Daniel Trottier

2.1 Introduction

> One case is related to a Scotch manufacturer, who rode after a sixteen years old runaway, forced him to return running after the employer as fast as the master's horse trotted, and beat him the whole way with a long whip. […] Other manufacturers were yet more barbarous, requiring many heads to work thirty to forty hours at a stretch, several times a week, letting them get a couple of hours of sleep only, because the night-shift was not complete, but calculated to replace a part of the operatives only. […] The consequences of these cruelties became evident quickly enough. The Commissioners mention a crowd of cripples who appeared before them, who clearly owed their distortion to the long working hours. This distortion usually consists of a curving of the spinal column and legs.[1]

This passage from Friedrich Engels' book *The Condition of the Working Class in England in 1844* describes typical working conditions in the phase of the industrialization of capitalism: work in factories was mentally and physically highly exhausting, had negative health impacts, and was highly controlled by factory owners and security forces.

> Our corporate headquarters, fondly nicknamed the Googleplex, is located in Mountain View, California. Today it's one of our many offices around the globe. While our offices are not identical, they tend to share some essential elements. Here are a few things you might see in a Google workspace: […]
>
> - Bicycles or scooters for efficient travel between meetings; dogs; lava lamps; massage chairs; large inflatable balls. […]

[1] Friedrich Engels, *The Condition of the Working Class in England in 1844* (Cambridge: Cambridge University Press, 1892/2010), 152.

C. Fuchs (✉) • D. Trottier
Department of Informatics and Media, Uppsala University, Kyrkogårdsgatan 10, Box 513, Uppsala 75120, Sweden
e-mail: christian.fuchs@im.uu.se; daniel.trottier@im.uu.se

S. Gutwirth et al. (eds.), *European Data Protection: Coming of Age*,
DOI 10.1007/978-94-007-5170-5_2, © Springer Science+Business Media Dordrecht 2013

- Foosball, pool tables, volleyball courts, assorted video games, pianos, ping pong tables, and gyms that offer yoga and dance classes.
- Grassroots employee groups for all interests, like meditation, film, wine tasting and salsa dancing.
- Healthy lunches and dinners for all staff at a variety of cafés.
- Break rooms packed with a variety of snacks and drinks to keep Googlers going (http://www.google.com/about/company/culture.html).

The work conditions in companies like Google are different than the ones described by Engels in the nineteenth century factory: the workplace seems at the same time to be a playground and an area for relaxation. But both Google and the nineteenth century Scotch manufacturer Engels described have one thing in common: they are profit-making companies that require a workforce to create economic value, and in turn need these value-creating activities to be secured.

Both also expect an intensive engagement from employees. This includes shifts that go beyond the modern standard of 8 h.[2] A discussion thread asked Google employees to describe their workday. Long hours were a constant complaint. One user said for example: I worked for the company for over 4 years before leaving. […] It's a competitive environment, though, and without good personal restraint things can really start to pile up. By the end my typical day was 14 h long and I was starting to underperform on my primary responsibilities. […]. The fast pace and competitive environment simply make it an easy trap for Googlers to fall into.[3] Another Google employee commented: "In terms of the work, I think it can be fast-paced and high-pressure [....]. Most of the people I know put in 50–60 hours a week....no one forces you to but to keep up, you almost sort of have to. That translates to a few late nights and maybe a few hours on the weekends".[4]

Both are aiming at maximal extraction from their employees: the former in order to maximize their engagement with machinery, physical labour, the latter in order to have fast turnarounds for software projects and ever-faster release dates. While foosball tables may seem preferable to physical beatings, both are efforts to totalize the worker's engagement with the company.

This chapter deals with the question of how workplace surveillance has changed in the age of the Internet. In order to provide an answer, we discuss the notion of workplace surveillance (Sect. 2.2), the emergence of play labour (Sect. 2.3), Internet play labour (Sect. 2.4), the surveillance of Internet play labour (Sect. 2.5), and finally the emergence of surveilled workplayplaces (Sect. 2.6).

[2] Ibid.

[3] http://www.reddit.com/r/AskReddit/comments/clz1m/google_employees_on_reddit_fire_up_your_throwaway/.

[4] Ibid.

2.2 Workplace Surveillance

This section aims to give a brief overview of important approaches for understanding workplace surveillance, such as the contributions by Karl Marx and Harry Braverman, discussions about Taylorism, and more recent examples.

For Karl Marx, surveillance of the workplace is a necessary element of capitalist production. He describes it as a function of capital: "The work of directing, superintending and adjusting becomes one of the functions of capital, from the moment that the labour under capital's control becomes co-operative. As a specific function of capital, the directing function acquires its own specific characteristics".[5] During the history of capitalism, work has become ever more distributed, social, and coordinated (more recent examples include the big stress on team work or the use of computer-supported in companies). Workplace surveillance (that is connected to and combined with workforce surveillance[6]) is a method that controls workers in order to ensure that they create value and that they create as much value as possible in their work time. Workplace surveillance is the surveillance of spaces, where work takes place (e.g. a factory space or office), it wants to make visible what happens in the social and physical spaces, where employees create value. Work time surveillance wants to make visible and measure the time span of the day an employee uses for productive activity, the speed of work, the sequence and durations of steps in the work process. Work takes place as activities in space and time that transform nature and culture and create goods and services that satisfy human needs. Work is productive transformative activity that takes place in space and time. It has a spatial and a behavioural aspect. Human behaviour always takes place in space. The surveillance of work is therefore necessarily surveillance of work places, work time, and workforces and these three dimensions are inherently connected.

Taylorism is the attempt to measure, monitor and control the bodily movements of workers in order to increase the value that is created during the work time.[7] It employs time studies, time study sheets, watch books, etc. in order to develop methods for optimizing production, i.e. the creation of more value in less time.

Harry Braverman described in his labour process theory the history of capitalism as a history of the control of the workforce. Technologies and methods like the assembly line, management, Taylorism, mechanization, automation and computerization would bring about capital's "control and dictation of each step of the process".[8]

Workplace surveillance is related to the capitalist production process, in which surplus value is generated.[9] It is the surveillance of the spaces where work is

[5] Karl Marx, *Capital. Volume I* (London: Penguin, 1867), 449.

[6] Christian Fuchs, "Political Economy and Surveillance Theory," op cit.

[7] Fredrick W. Taylor, *The Principles of Scientific Management* (New York: Harper, 1911).

[8] Harry Braverman, *Labor and Monopoly Capital* (New York: Monthly Review Press, 1974), 69.

[9] For a detailed discussion of how various forms of surveillance relate to the capital accumulation process, see: Fuchs, "Political Economy and Surveillance Theory," *Critical Sociology* 38 (2012, forthcoming).

conducted to ensure that workers conduct the duties that have been assigned to them and create value. Workplace surveillance aims at ensuring that employees do not use work time as idle time, but as surplus value-generating activity. Workforce surveillance is surveillance of the activities of employees. It includes performance measurement and activity assessment, and aims at creating data for making the work process more efficient, i.e., producing more surplus value in less time. Both forms can either be known or unknown to the employees. Known workplace and workforce surveillance makes employees discipline their own activities. Covert workplace surveillance aims at detecting employees that are considered to be unproductive or it acts as data foundation to make organizational changes (such as promotion of the most loyal and efficient employees, lay-off of employees that are considered as not productive enough). This surveillance either remains unknown or becomes known only later to employees.

Forms of workforce and workplace surveillance include the use of slave masters in slaveholder societies and foremen and overseers in factories in industrial societies. There are also more technologically mediated forms like work time control systems (ranging from punch card systems to automated digital systems), the use of CCTV or workflow management systems.

Lidl is one of the largest discount food store chains in Germany. In 2008 it became known that it used detectives and CCTV cameras for monitoring how often employees go to the toilet, how well the work is performed, which employees have intimate relations, what conversations between employees are about, etc. The results of these surveillance processes were documented in reports. *Stern* journalist Malte Arnsperger stated: "Lidl seems to try to know about its employees as much as possible, many details, so to have means of pressure available if one wants to dismiss them, if one […] maybe does not want to make salary increases, if one wants to carry out salary cuts. It is basically about means for exerting pressure on employees".[10] In this example, workplace surveillance seems to have aimed at putting pressure on employees in order to accept wage cuts and make them create more surplus value in less time. It was unknown to the employees that they were the objects of surveillance and that the surveillance measures were not aimed at potential thieves.

Workplace and workforce surveillance technologies are means of class struggle by employers that are used for trying to strengthen capital's power against workers, lowering wage costs and increasing absolute and relative surplus value production. Absolute surplus value production means, according to Marx,[11] that employees work longer time (e.g. by reducing breaks or conversations with colleagues during work time because they are afraid of being monitored and losing their job). In relative surplus value production, employees work more in the same time, i.e., they create more surplus value than at earlier points of time in the same or shorter time spans.[12]

[10] Translation from German. Überwachung bei Lidl: So wurde der Spitzelskandal aufgedeckt, Stern Online, 25.3.2008, http://www.stern.de/panorama/ueberwachung-bei-lidl-so-wurde-der-spitzelskandal-aufgedeckt-615056.html. Accessed on March 21st, 2012.

[11] Marx, op cit, Chap. 12.

[12] Marx, op cit, Chap. 12.

Capitalism is necessarily based on economic surveillance. But surveillance methods are older than capitalism. The slave master who monitors the work of a slave in an ancient slaveholder society is a symbol for the connection of surveillance to any form of exploitation. We can therefore say that economic surveillance is as old as the division of labour and the associated power differentials. Surveillance is older than capitalism, was incorporated into capitalism as a functional principle and was thereby also transformed.

In classical forms of workforce control, the monitoring of work tends to be experienced by the worker as a form of alienation. In classical industrial work there is also a clear separation between work time and non-work time, alienated labour time and non-alienated free time.[13] Classical critical studies of workplace surveillance have stressed that "the subsequent history of capitalist industry […] has been a matter of the deepening and extension of information gathering and surveillance to the combined end of planning and control".[14] In order to understand, how workplace and workforce surveillance have gained new qualities in the age of the Internet, we need to discuss changes that the organization of labour has been undergoing.

Given the discussion of classical workplace and workforce surveillance, we will discuss next some more recent changes of how labour is organized.

2.3 The Rise of Play Labour

Luc Boltanski and Éve Chiapello argue that the rise of participatory management means the emergence of a new spirit of capitalism that subsumes the anti-authoritarian values of the political revolt of 1968 and the subsequently emerging New Left such as autonomy, spontaneity, mobility, creativity, networking, visions, openness, plurality, informality, authenticity, emancipation, and so on, under capital. The topics of the movement would now be put into the service of those forces that it wanted to destroy. The outcome would have been "the construction of the new, so-called 'network' capitalism"[15] so that artistic critique – that calls for authenticity, creativity, freedom and autonomy in contrast to social critique that calls for equality and overcoming class[16] – today "indirectly serves capitalism and is one of the instruments of its ability to endure".[17]

[13] Marxist Feminsm has stressed that also the free time is not alienation-free: Especially for women the household economy of the family means alienated and unpaid work that reproduces labour power of wage workers in the family.

[14] Kevin Robins and Frank Webster, *Times of Technoculture: From the Information Society to the Virtual Life* (London: Routledge, 1999): 245.

[15] Luc Boltanski and Eve Chiapello, *The New Spirit of Capitalism* (London: Verso, 2007), 429.

[16] ibid, 37 f.

[17] ibid, 490.

Boltanski and Chiapello stress that the network concept (that points towards management's emphasis on semi-autonomous work groups, work time flexibilization, the flattening of organizational hierarchies, the development of organizational philosophies, outsourcing and globalization of organizations, etc.) has become a new ideology for justifying capitalism. In addition, it contributes to new forms of work control. Gilles Deleuze[18] has in this context pointed out that Foucauldian disciplinary power has been transformed in such a way that humans increasingly discipline themselves without direct external violence. He terms this situation the society of (self-)control. Deleuze compares the individual in disciplinary society to a mole and the individual in the society of control to a serpent. The mole as a symbol of disciplinary society is faceless and dumb and monotonously digs his burrows; the snake is flexible and pluralistic. The Google worker is a serpent: s/he flexibly switches between different activities (leisure, work) so that the distinction between leisure and work, play and labour, collapses. Being employed by Google means having to engage in Google labour life and Google play life. At Google (and similar companies), it becomes difficult to distinguish play and work.[19] One can therefore talk about the emergence of play labour (playbour).

Participatory management promotes the use of incentives and the integration of play into labour. It argues that work should be fun, workers should permanently develop new ideas, realize their creativity, enjoy free time within the factory, etc. The boundaries between work time and spare time, labour and play, become fuzzy. Work tends to acquire qualities of play, whereas entertainment in spare time tends to become labour-like. Work time and spare time become inseparable. At the same time work-related stress intensifies and property relations remain unchanged.[20]

There is a tendency in contemporary capitalism that in some companies and in the organizaton of life the boundaries between play and work collapse. During Fordist capitalism, there was a clear separation between work time and spare time. Spare time to a certain extent was the time of play, where one did not have to be productive. At the same time, spare time was the reproduction time of labour power and involved labour-related activities like housework so that industrial logic also shaped spare time and pleasure was administered pleasure and organized spontaneity in consumer society. So spare time was never really free time in capitalism, but it was easier to find spaces for non-productive and non-labour activities. We can distinguish between instances where leisure comes to resemble work (workification of play) and instances where work comes to resemble leisure (the playification of work). Examples for the workification of play include: extreme sports as free time

[18] Gilles Deleuze, "Postscript on the Societies of Control," in *Negotiations* (New York, NY: Columbia University Press, 1995), 177–82.

[19] Christian Fuchs, "A Contribution to the Critique of the Political Economy of Google," *Fast Capitalism* 8 (2011, 1).

[20] Mike Parker and Jane Slaughter, "Unions and Management by Stress" in *Lean Work: Empowerment and Exploitation in the Global Auto Industry*, ed. Steven Babson (Detroit, MI: Wayne State University Press, 1995), 41–53.

activity, the emergence of trade structures in computer games (the selling of avatars that are created and developed by cheap workers – called gold farmers – in developing countries), the recruitment of soldiers with the help of computer games such as America's Army, fantasy football leagues, substitution of idleness by performance-based activities, industries of administered idleness (slow food cooking courses, spas, massages, meditation, etc.).

Examples of the playification of work include: the performance of work tasks while commuting or during formal spare time via mobile phones, mobile Internet and laptops; the integration of recreational possibilities (as e.g. sports facilities) and social activities into the work place, having love for the job in creative work that results in high performance and work dedication, smart phones among employees as an electronic 'toy' that extends work responsibilities into leisure time; 'Barcamps', happy hours and 'unconferences' are examples of seemingly social gatherings after work hours, where employees are expected to 'network' on behalf of their company to obtain new clients, promote their brand, and otherwise turn even social life into labour.

Capitalism connects labour and play in a destructive dialectic. Under Fordist capitalism, play in the form of enjoyment, sex, and entertainment was in capitalism only part of spare time, which was unproductive and separate from labour time. Freud argued that the structure of drives is characterized by a dialectic of Eros (the drive for life, sexuality, lust) and Thanatos (the drive for death, destruction, aggression).[21] Humans according to Freud strive for the permanent realization of Eros (pleasure principle), but culture would only become possible by a temporal negation and suspension of Eros and the transformation of erotic energy into culture and labour. Labour would be a productive form of desexualisation – the repression of sexual drives. Freud speaks in this context of the reality principle or sublimation. The reality principle sublates the pleasure principle. Human culture thereby sublates human nature and becomes man's second nature.

Marcuse in his book *Eros and Civilization* connected Freud's theory of drives to Marx's theory of capitalism. He argued that alienated labour, domination, and capital accumulation have turned the reality principle into a repressive reality principle – the performance principle: alienated labour constitutes a surplus-repression of Eros. The repression of the pleasure principle takes on a quantity that exceeds the culturally necessary suppression. Marcuse connected Marx's notions of necessary labour and surplus labour/value to the Freudian drive structure of humans and argued that necessary labour on the level of drives corresponds to necessary suppression and surplus labour to surplus-repression. Necessary labour is the average amount of hours people need to work annually in a society in order to guarantee the survival of this society and the people living in it by creating goods and services that satisfy basic human needs. This means that individuals in society have for a certain share of hours per year to engage in productive work and during this time have to suppress

[21] Sigmund Freud, *Beyond the Pleasure Principle* (New York: Norton, 1961).

their desires for pleasure (=necessary suppression of the pleasure drive that accompanies necessary labour). This means that in order to exist, a society needs a certain amount of necessary labour (measured in hours of work) and hence a certain corresponding amount of suppression of the pleasure principle (also measured in hours). The exploitation of surplus value (labour that is performed for free and generates profit) results not only in the circumstance that workers are forced to work for free for capital to a certain extent, but also in the circumstance that the pleasure principle must be additionally suppressed.

"Behind the reality principle lies the fundamental fact of Ananke or scarcity (*Lebensnot*), which means that the struggle for existence takes place in a world too poor for the satisfaction of human needs without constant restraint, renunciation, delay. In other words, whatever satisfaction is possible necessitates work, more or less painful arrangements and undertakings for the procurement of the means for satisfying needs. For the duration of work, which occupies practically the entire existence of the mature individual, pleasure is 'suspended' and pain prevails".[22] In societies that are based domination, the suppression and postponement of pleasure gratification takes on the form of the so-called "performance principle",[23] according to which pleasure gratification is only allowed as long as it does not interfere or diminish the productivity of the worker.

In societies that are based on the principle of domination, the reality principle takes on the form of the performance principle: Domination "is exercised by a particular group or individual in order to sustain and enhance itself in a privileged situation".[24] The performance principle is connected to surplus-repression, a term that describes "the restrictions necessitated by social domination".[25] Domination introduces "additional controls over and above those indispensable for civilized human association".[26]

Marcuse argues that the performance principle means that Thanatos governs humans and society and that alienation unleashes aggressive drives within humans (repressive desublimation) that result in an overall violent and aggressive society. Due to the high productivity reached in late-modern society, a historical alternative would be possible: the elimination of the repressive reality principle, the reduction of necessary working time to a minimum and the maximization of free time, an eroticization of society and the body, the shaping of society and humans by Eros, the emergence of libidinous social relations. Such a development would be a historical possibility – but one incompatible with capitalism and patriarchy.

Kücklich first introduced in this context the term playbour (play + labour).[27] In the Fordist mode of capitalist production, work time was the time of pain and the

[22] Marcuse, op cit, 35.

[23] ibid, 35 ff.

[24] ibid, 36.

[25] ibid, 35.

[26] ibid, 37.

[27] Julian Kücklich, "Precarious Playbour," *Fibreculture Journal* 5.

time of repression and of the human drive for pleasure; whereas leisure time was the time of Eros and pleasure.[28] In contemporary capitalism, play and labour, that is Eros (the pleasure principle) and Thanatos (the death drive) partially converge: workers are expected to have fun during work time and play time becomes productive and work-like. Play time and work time intersect and all available time tends to be exploited for the sake capital accumulation.

The difficulty is that labour feels like play and that exploitation and fun thereby become inseparable. Play and labour are today in certain cases indistinguishable. Eros has become fully subsumed under the repressive reality principle. Play is largely commodified, spaces and free time that are not exploited by capital hardly exist today. They are difficult to create and to defend. Play today is productive, surplus value generating labour that is exploited by capital. All human activities, and therefore also all play, tends under the contemporary conditions to become subsumed under and exploited by capital. Play as an expression of Eros is thereby destroyed, human freedom and human capacities are crippled.

The emergence of playbour does not replace Fordist and industrial forms of work that are based on the separation of labour time and reproductive spare time. It is a new quality of the organization of work that is connected to the rising importance of knowledge and creative work and the attempts of capital to overcome crises by reorganizing work. In playbour, surveillance as coercive means of work control is substituted or complemented by ideological forms of control, in which workers monitor and maximize their own performance or monitor themselves mutually. Surveillance thereby becomes transformed into control of the self. Playbour is a biopolitical form of ideology and control.

Biopolitics means that "basic biological features of the human species" are "the object of a political strategy, of a general strategy of power".[29] "Biopower […] refers to a situation in which what is directly at stake in power is the production and reproduction of life itself".[30] Playbour is an actual control strategy of humans that aims at enhancing productivity and capital accumulation. At the same time, it is an ideology that postulates (e.g. in management ideology, public debates, etc.) the democratization of work and thereby wants to create the illusionary impression that we have entered an age without alienation and exploitation.

Playbour is a context for the discussion of changes of the role of mediated surveillance on the Internet.

---

[28] Herbert Marcuse, *Eros and Civilization* (Boston, MA: Beacon Press, 1955).

[29] Michel Foucault, *Security, Territory, Population. Lectures at the Collège de France 1977–1978* (Basingstoke: Palgrave Macmillan, 2007), 1.

[30] Hardt, Michael and Antonio Negri, *Empire* (Cambridge, MA: Harvard University Press, 2000), 24.

2.4 Internet Playbour

In the so-called *Blindspot Debate*, Dallas Smythe[31] asked the question what the commodity sold by the commercial media is. He argued that they do not primarily sell content, but the audience as a commodity to advertisers. The consumption of commercial media would be a value-creating and productive activity. Smythe coined in this context the notion of the audience commodity. He argued that if media consumption becomes productive, spare time becomes work time: The "material reality under monopoly capitalism is that all non-sleeping time of most of the population is work time. […] Of the off-the-job work time, the largest single block is time of the audiences which is sold to advertisers. […] In 'their' time which is sold to advertisers workers (a) perform essential marketing functions for the producers of consumers' goods, and (b) work at the production and reproduction of labour power".[32] Sut Jhally and Bill Livant have pinpointed Smythe's concept of audience commodification by saying that it means: "watching as working".[33]

If one assumes that also sleeping time is related to work time because it is an activity that reproduces and recreates labour power, then one can argue that for "the great majority of the population […] 24 hours a day is work time".[34] Media consumption is audience work that creates value for media companies. The result of this work is the presentation of commodities to audiences in advertisements. Therefore audiences "work to market […] things to themselves".[35]

Dallas Smythe suggests that in the case of media advertisement models, the audience's attention time is sold as a commodity to advertisers (audience commodity). Although the commercial mass media audience that Smythe described (typically found in the case of advertising-financed newspapers, radio, and TV) creates value by watching or reading, it does not create content itself. Commercial surveillance in this model is externally imposed by market and audience research (e.g. by using set top boxes that measure audience activities). The audience is measured by special methods that are not applied to the full audience, but to a sample of study participants. Audience measurement is used for setting advertising rates. It is necessarily based on approximations.

Internet platforms such as Google, Facebook, YouTube and Twitter share with commercial newspapers and commercial broadcasting the profit orientation and the focus on advertising-generated revenue. The difference is that users on these platforms create and share content, establish and maintain social relations (communication), and that

[31] Dallas W. Smythe, "Communications: Blindspot of Western Marxism," *Canadian Journal of Political and Social Theory* 1 (1977, 3): 1–27.

[32] ibid, 3.

[33] Sut Jhally and Bill Livant. "Watching as Working. The Valorization of Audience Consciousness," in *The Spectacle of Accumulation. Essays in Culture, Media, & Politics* (New York: Peter Lang, 1986/2006), 125.

[34] Dallas W. Smythe, *Dependency Road* (Norwood, NJ: Ablex, 1981), 47.

[35] ibid, 4.

surveillance is built into the system as internal mechanism that records, monitors, and assesses all generated content, social relations, and transaction data. Thereby a full profile of user interests, connections and activities emerges that is not limited to audience samples, but encompasses the total surveillance of all user activities. The totality of commercial surveillance on the Internet enables targeted advertising – advertising that is oriented on individual user preferences, relations and activities.

Audience commodification on the corporate Internet can best be described as Internet prosumer commodification[36]: economic surveillance on corporate social media is surveillance of prosumers, who create and share user-generated content, browse profiles and data, interact with others, join, create, and build communities, and co-create information. The conflict between Cultural Studies and Critical Political Economy of the Media[37] about the question of the activity and creativity of the audience has been resolved in relation to the Internet today: On Facebook, Twitter, commercial blogs, etc., users are fairly active and creative, which reflects Cultural Studies' insights about the active character of recipients, but this active and creative user character is the very source of exploitation, which reflects Critical Political Economy's stress on class and exploitation.

Internet prosumer commodification signifies that private internet usage, which is motivated by play, entertainment, fun, and joy – aspects of Eros – has become subsumed under capital and has become a sphere of the exploitation of labour. Internet corporations accumulate profit by exploiting the playbour of users. In playbour time, surplus value generation appears to be pleasure-like, but serves the logic of repression (the lack of ownership of capital). Joy and play become toil and work, toil and work feel like joy and play. There is a collapse of leisure time and work time: leisure time becomes work time and work time leisure time. All time becomes exploited, online leisure time becomes surplus value-generating wage labour time that involves a surplus repression time of pleasure. Playbour time is surplus value generating pleasure time.

In commercial Internet surveillance, users work without pay and produce content, communications, social relations, and transaction data. Their unpaid labour creates data commodities (collection of individuals with specific user demographics) that are sold to advertisers. There is an exchange of money with access to specific user groups. The exchange value of the Internet prosumer commodity is at the heart of targeted advertising. This commodity's value is created by playbour – the activities on Facebook and related platforms are strongly playful activities

[36] Christian Fuchs, "Labor in Informational Capitalism and on the Internet," *The Information Society* 26 (2010, 3): 179–96.

[37] For the discussion between Cultural Studies and Critical Political Economy of the Media & Comunication see: Marjorie Ferguson and Peter Golding, ed. *Cultural Studies in Question* (London: SAGE, 1997). Nicholas Garnham, "Political Economy and Cultural Studies: Reconciliation or Divorce?" in *Cultural Theory and Popular Culture*, ed. John Storey (Harlow: Pearson, 1995/1998), 600–12. Lawrence Grossberg, "Cultural Studies vs. Political Economy. Is Anybody Else Bored with this Debate?" in *Cultural Theory and Popular Culture*, ed. John Storey (Harlow: Pearson, 1995/1998), 613–24.

conducted in all places at all times. They hardly feel like labour, but create economic value. Permanent real time surveillance is a feature of many forms of Internet playbour.

2.5 Internet Surveillance

In order to understand, how Internet surveillance and the surveillance of Internet playbour work, we first need a model that explains the human information process. One such model is based on Hegelian dialectical philosophy, which allows us to identify three levels/stages of social life: cognition, communication and co-operation[38] (Fuchs 2008, 2010a, b). This model is dialectical because it corresponds to the three stages of the dialectical logic identified by Hegel: identity/being-in-itself, being-for-another, being-in-and-for-itself. Abstractly speaking, any entity in the world is unique, although it is one of a kind, it is identical with itself (I=I). But an entity does not exist as a monad in the world, it can only exist in relation to another entity. So being is always relational being, one entity exists in difference and relation to others, existence is individual and relational at the same time (being-for-another, contradiction, negation). Out of the relation between entities, new qualities can emerge. This is not an automatic necessity, but always a potentiality. Hegel describes the process of the emergence of new qualities as Aufhebung (sublation) or negation of the negation. In society, this model of dialectical logic can be applied to the existence of humans. One stage is the precondition for the next. First, the individual, who acts through cognition. Second, individuals engage in social relations through communication. Third, relational communication contributes to cooperative endeavours and/or community building/maintenance. Organisations and communities are produced and reproduced at this final stage. The three stages correspond to three notions of sociality: Emile Durkheim's social facts (cognition), Max Weber's social action (communication), Ferdinand Tönnies' concept of community as well as Karl Marx's notion of collaborative work (co-operation).[39] Both community and collaborative work are expression of co-operation.

This is the structural basis of social life. Individual action is the basis of communication, which in turn is the basis of corporate endeavours as well as community building. Media has always played an important role in these stages. Because it turns thought into digital content, and transmits that content to other users, all media technologies have played a crucial role in these functions.

[38] Christian Fuchs, *Internet and Society. Social Theory in the Information Age* (New York: Routledge, 2008). Christian Fuchs, "Social Software and Web 2.0: Their Sociological Foundations and Implications," in *Handbook of Research on Web 2.0, 3.0, and X.0: Technologies, Business, and Social Applications, Volume II*, ed. San Murugesan (Hershey, PA: IGI-Global, 2010), 764–89.

[39] Ibid.

What is unique about social media is the fact that it collapses these three processes together. Individual cognition almost automatically becomes a matter of social relations, and a cooperative endeavour. For instance, I may write a reflexion on my profile. By default, other users will see this reflexion, and be able to respond to it. The reflexion becomes a statement towards others, and also becomes a project. If I wrote this statement on a word processor, it would remain in the first stage. If I wrote this statement on a conventional website, it would remain in the second stage.

The ease with which it moves through these social stages is not entirely new. But what is striking about social media – indeed, what makes it a convergence of the three modes of sociality – is the difficulty of remaining in the first or second stage. By virtue of its built-in functionality, individual thought becomes relational and cooperative. Self-reflexion now exists in a relational sense (it has an audience, it is sent to that audience), and it also becomes a kind of cooperative activity (that audience is expected to contribute to that initial reflexion). So for example writing a blog post or a Facebook wall post is a form of self-reflexion that at the same time is outreaching to a community and by way of comments of this community is shaped by others' ideas.

Social media makes reflection and communication a complex form of sociality by pushing both of these towards a cooperative stage. This has specific implications for both visibility and labour. In terms of visibility, content that would otherwise stay with an individual is by default pushed to a broad audience. Any content that is uploaded to a site like Facebook (on the profile, excluding the private message) is sent to that person's entire social network. It may possibly be sent beyond this network if their privacy settings are relaxed.

Something can remain cognition by not being put on Facebook. While this is true, this either-or approach differs from other media. The word processor keeps the content with the individual, who may decide to print or transmit the content. Even the email allows you to save a draft before sending it to others. Yet with social media the only option is to publish.

Social media pushes activity into the realm of labour by making it visible (as seen above) and collaborative, no matter if it is an intentional act of communication or an act of browsing. Everything becomes an entry point to a comment. Users are positioned vis-à-vis one another, obliged to intake what others produce, and produce a response. Statements become conversations; there is no final word. Photographs and videos become conversations. News items linked from an outside site become conversations. With social advertising schemes, conversations about products in a community of friends and contacts are invited by the ad mechanism itself on a digital platform with the help of the constant monitoring of online behaviour, purchasing patterns and the social networks/relations of users. Social advertising is based on the gathering, analysis, and comparison of online behaviour and the predictive algorithmic calculation of potential purchasing choices.

Social saturation contributes to its value for companies, and its potential for exploitation. It is not only that cognition can become cooperation, but the specific status and location of sites like Facebook, especially for individual users. They frame their functionality in a very generic light. They are simply designed to 'share'

with the 'people' that 'matter' to you. They are therefore cross-contextual, or rather they contribute to a convergence of social contexts. They monopolize the user's social life.

Modern society is based on the differentiation of social roles. In modern society, human beings act in different capacities in different social roles. Consider the modern middle-class office worker, who also has roles as a husband, father, lover, friend, voter, citizen, child, fan, neighbour, to say nothing of the various associations to which he may belong. In these different roles, humans are expected to behave according to specific rules that govern the various social systems of which modern society is composed (such as the company, the schools, the family, the church, fan clubs, political parties, etc.).

Jürgen Habermas[40] describes how modern society is grounded in different spheres, in which humans act in different roles. He says that modernity resulted in:

(a) the separation of the economy from the family and the household so that the modern economy (based on wage labour and capital) emerged,
(b) the rise of a political public sphere, in which humans act as citizens, who vote, hold a political opinion, etc., in contrast to the earlier monarchic system, in which political power was controlled by the monarch, aristocracy, and the church. This includes the shift of the economy towards a capitalist economy grounded in private ownership of the means of production and on the logic of capital accumulation. The economy started to no longer be part of private households, but became organized with the help of large commodity markets that go beyond single households. The modern economy has become "a private sphere of society that […] [is] publicly relevant"[41] The family started to no longer be primarily an economic sphere, but the sphere of intimacy and the household economy based on reproductive labour. Connected to this was the separation of the private and the public sphere that is based on humans acting in different roles.[42] Habermas mentions the following social roles that are constitutive for modern society: employee, consumer, client, citizen.[43] Other roles, as e.g. wife, husband, houseworker, immigrant, convicts, etc. can certainly be added. So what is constitutive for modern society is not just the separation of spheres and roles, but also the creation of power structures, in which roles are constituted by power relations (as e.g. employer-employee, state bureaucracy-citizen, citizen of a nation state-immigrant, manager-assistant, dominant gender roles – marginalised gender roles).

[40] Jürgen Habermas, *The theory of communicative action. Volume 2: Lifeworld and system: a critique of functionalist reason* (Boston, MA: Beacon Press, 1987). Jürgen Habermas. *The structural transformation of the public sphere* (Cambridge, MA: MIT Press, 1989).

[41] Jürgen Habermas. *The structural transformation of the public sphere,* op cit, 19.

[42] ibid. 152, 154. See also Hannah Arendt, *The human condition*. (Chicago: University of Chicago Press, 1958), 47, 68. 2nd edition.

[43] Jürgen Habermas, *The theory of communicative action. Volume 2: Lifeworld and system: a critique of functionalist reason* (Boston, MA: Beacon Press, 1987), 320.

With social media, the constitutive features are the following:

- *Integrated sociality*: The convergence of the three modes of sociality (cognition, communication, cooperation) in an integrated sociality. This means for example on Facebook, and individual creates a multi-media content like a video on the cognitive level, publishes it so that others can comment (the communicative level), and allows others to manipulate and remix the content, so that new content with multiple authorship can emerge. One step does not necessarily result in the next, but the technology has the potential to enable the combination of all three activities in one space. Facebook, by default, encourages the transition from one stage of sociality to the next, within the same social space.
- *Integrated roles*: Social media like Facebook are based on the creation of personal profiles that describe the various roles of a human being's life. In contemporary modern society, different social roles tend to converge in various social spaces. The boundaries between public life and private life as well as the work place and the home have become fuzzy and liquid. A new form of liquid and porous sociality has emerged, in which we partly act in different social roles in the same social space. On social media like Facebook, we act in various roles, but all of these roles become mapped onto single profiles that are observed by different people that are associated with our different social roles. This means that Facebook is a social space, in which social roles tend to converge and become integrated in single profiles.
- *Integrated and converging surveillance on social media*: On social media like Facebook, various social activities (cognition, communication, co-operation) in different social roles that belong to our behaviour in systems (economy, state) and the lifeworld (the private sphere, the socio-economic sphere, the socio-political sphere, the socio-cultural sphere) are mapped to single profiles. In this mapping process, data about a) social activites within b) social roles are generated. This means that a Facebook profile holds a1) personal data, a2) communicative data, a3) social network data/community data in relation to b1) private roles (friend, lover, relative, father, mother, child, etc.) b2) civic roles (socio-cultural roles as fan community members, neighbourhood association members, etc). b3) public roles (socio-economic and socio-political roles as activists and advocates), b4) systemic roles (in politics: voter, citizen, client, politician, bureaucrat, etc.; in the economy: worker, manager, owner, purchaser/consumer, etc.). The different social roles and activities tend to converge, as e.g. in the situation where the workplace is also a playground, where friendships and intimate relations are formed and dissolved and where spare time activities are conducted. This means that social media surveillance is an integrated form of surveillance, in which one finds surveillance of different (partly converging) activities in different partly converging social roles with the help of profiles that hold a complex networked multitude of data about humans.

Figure 2.1 visualizes the surveillance process on one single social media system (such as Facebook, etc.). The total social media surveillance process is a combination and network of a multitude of such processes.

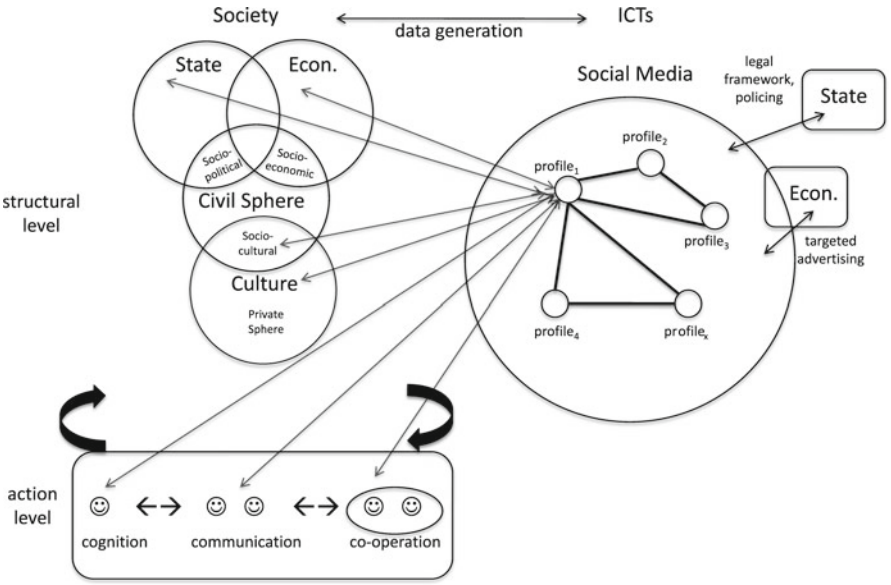


Fig. 2.1 The process of social media surveillance

Social media is made up of voluntary and involuntary forms of exposure and information exchange. Users rely on social media for social and cultural life. These activities are made visible to social media companies like Facebook, and by extension to whomever these companies wish to sell this data.

Communication occurs within, but also across different social actors. This is often voluntary, but surveillance underscores when information is obtained in a manner that is involuntary by the sender. One aspect of social media surveillance is the mutual augmentation of surveillance,[44] which dictates that the coexistence of so many social actors on one media platform means that users will have access to so much more information from other social actors. Thus, any attempt to gather information will be augmented by the visibility of so many other social relations. Voluntary visibility augments involuntary visibility.

Surveillance of Internet users includes:

- surveillance of personal profile data,
- surveillance of produced content,
- surveillance of browsing and clicking behaviour,
- surveillance of social relations and networks,

[44] Daniel Trottier, *Social media as surveillance* (Farnham: Ashgate, 2012).

- surveillance of communication.

The hybrid of play and labour is apparent in the case of social media surveillance. This activity is framed in terms of "sharing" and "connecting". Friends and colleagues are placed in the foreground, and the value-adding process and business outcomes are obscured. Yet this activity is intercepted, gathered, and monitored, part of the process by which social activity on social media is transformed into a commodity.

The legal mechanism that enables the exploitation of social media users are privacy policies and terms of use. Surveillance of user activities for the purpose of selling targeted advertisements is legally guaranteed by these policies. Facebook, the major social networking site and the second most popular web platform in the world, says in its data use policy: "When an advertiser creates an ad on Facebook, they are given the opportunity to choose their audience by location, demographics, likes, keywords, and any other information we receive or can tell about you and other users. […] Sometimes we get data from our advertising partners, customers and other third parties that helps us (or them) deliver ads, understand online activity, and generally make Facebook better".[45]

Facebook avoids the term selling and instead speaks of "getting" and "sharing" user data, just as users "share" with other users. Both interpersonal communication and exploitative labour are collapsed into the same term. The terms "sell" and "selling" do not appear once in the policy that legitimates the surveillance of user activities and the selling of their data as commodity, whereas the term sharing appears 59 times in the 6,911 word long policy.

There are two connections of social media surveillance to the topic of workplace surveillance.

1. *Corporate social media* are a *surveilled workplayplace*.
   When using corporate social media, users engage in value-creating labour that is constantly monitored and feels like play.
2. Facebook and other *social media* are used as *technologies for the surveillance of wage labour* in conventional workplaces.
   The matching of different roles and activities into roles onto single profiles enables employers to gain insights into a lot of details of the lives of their employees. It has become a common practice that companies check job candidates' social media profiles, which constitutes a new form of applicant surveillance. A survey showed that in 2009 45% of US companies used social media for applicant surveillance.[46]

In the case of employer-employee relations, new issues arise: What to do if your boss befriends you on Facebook? Should private Facebook use be allowed at the

[45] https://www.facebook.com/full_data_use_policy, version from September 23, 2011.

[46] Jenna Wortham, 'More employers use social networks to check out applicants', The New York Times Bits Blog, August 20 2009, available at http://bits.blogs.nytimes.com/2009/08/20/more-employers-use-social-networks-to-check-out-applicants/.

workplace? What to do if your company asks you to use your private social media profiles for promoting their products, services, or events? Should there be Facebook groups for individual companies, on which employees, managers, etc. connect? All of these questions indicate the circumstance that the boundaries between private life and working life have become porous. This circumstance can pose problems because although social media are networked spaces, workplaces are enmeshed into and shaped by power structures, in which employees and managers have an asymmetrical share of authority and influence. Social media are technologies that help extending workplace surveillance into realms that were previously thought to be autonomous, but now become increasingly subsumed under the gaze of capital and management.

The use of social media (especially social networking sites like Facebook) as tools of applicant and workforce surveillance is a relatively new area of research and concern.[47] The published works on this topic[48] tend to agree that this issue is legally relatively unregulated and that more social scientific and legal research is needed in this area.

Sánchez Abril, Levin and Del Riego argue that "employer intrusion into an employee's personal life threatens the employee's freedom, dignity, and privacy – and may lead to discriminatory practices".[49] They conducted a survey, in which 2,500 undergraduate students participated and found that 71% agreed that the following scenario could result in physical, economic, or reputational injury in the offline world[50]: "You called in sick to work because you really wanted to go to your friend's all day graduation party. The next day you see several pictures of you having a great time at the party. Because the pictures are dated you start to worry about whether you might be caught in your lie about being sick. You contact the developers of the social network and ask that the pictures be taken down because the tagging goes so far, it would take you too long to find all the pictures. There was no response from the network. You are stunned to be called in by your supervisor a week later to be advised that you were being 'written up' for taking advantage of sick leave and put on notice that if it happened again you would be terminated".[51]

---

[47] See: Leigh A. Clark and Sherry J. Roberts. 2010. "Employer's Use of Social Networking Sites: A Socially Irresponsible Practice." *Journal of Business Ethics* 95 (4): 507–525. Kristl H Davison, Catherine Maraist, R.H. Hamilton and Mark N. Bing. 2012. "To Screen or Not To Screen? Using The Internet For Selection Decisions." *Employee Responsibilities and Rights Journal* 24 (1,): 1–21. Kristl H Davison, Catherine Maraist and Mark N. Bing. 2011. "Fiend or Foe? The Promise and Pitfalls of Using Social Networking Sites for HR Decisions." *Journal of Business and Psychology* 26 (2): 153–159. Patricia Sánchez Abril, Avner Levin and Alissa Del Riego. 2012. "Blurred Boundaries. Social Media Privacy and the Twenty-First-Century Employee." *American Business Law Journal* 49 (1): 63–124.

[48] Ibid.

[49] Sánchez Abril, Levin and Del Riego, op cit, 69.

[50] ibid, 104 f.

[51] ibid, 104.

[52] Clark and Roberts, op cit, 518.

Clark and Roberts argue that notwithstanding all legal debates, employer's monitoring of employees' or applicants' social networking sites profiles is a socially irresponsible practice because in such practices allow "employers to be undetectable voyeurs to very personal information and make employment decisions based on that information",[52] such monitoring can due to the persistence of online information have negative career effects that impact a whole working life, and employment decisions can become based on very sensitive information that are inappropriate values for decision making in the economy ("she is too conservative or too liberal; 'she is a sinner for sexual preference'"[53]).

Protecting employees and job applicants from decisions being made based on information derived from social media is important because there is an asymmetrical power relationship between employers and managers on the one hand and employees and applicants on the other side. There is a class relationship, i.e. an asymmetric power structure of the capitalist economy, in which employers and companies have the power to determine and control many aspects of the lives of workers and consumers. Given the power of companies in the capitalist economy, economic privacy needs to be contextualized in a way that protects consumers and workers from capitalist control and at the same time makes corporate interests and corporate power transparent. The existence of this asymmetrical power relationship, in which employers can decide if employees are hired and fired, requires special protection of workers and applicants. It is therefore an interesting question for policy makers if basing employment and lay-off decisions on information obtained from social media should be outlawed and if companies engaging in such practices should face severe penalties.

2.6 Conclusion: The Surveilled Workplayplace Factory

We encountered various examples of the surveillance of workers in this paper: Engels described the brutal physical beating and control of workers in the UK in the 1840s. Taylorism and Fordism made use of the conveyor belt line and scientific management to control workers. Employees at Lidl have been monitored by CCTV. Internet prosumers activities are monitored and commodified in real time by companies like Google and Facebook. Workers in developing countries are working long hours and are facing sanctions, threats, and permanent observation of their work.

All of these forms of surveillance have in common that they aim at the control of workers' activities in order to accumulate a maximum of capital with the least expenses and as quickly as possible. The history of capitalism is also a history of the development of methods of exploitation and workers' control. The forms of economic surveillance did not supplant older ones, but rather complemented them and added new dimensions. Physical surveillance that includes beatings, whipping,

[53] ibid, 51.

sanctions, etc. was complemented by a form of control that is built into production technology (e.g. the conveyor belt) and dictates the speed and organization of work. In twentieth century, the role of the manager as organizer and controller of the work process emerged. Management has developed many different methods (ranging from overt control to "participatory management") that are all focused on ensuring that employees work, work more intense, and to contain and foreclose workers struggles. The rise of Fordist mass consumption and mass production brought about the rise of consumer surveillance: various methods of consumer and advertising research were developed for studying, measuring, controlling, and creating consumer needs. Twentieth century saw also the rise of computing and the diffusion of computing into surveillance technologies that increasingly became digital, automated, and networked. The bureaucratic file turned into digital database sets, the punch time card into networked monitoring. The rise of Internet use has extended and intensified the rise of productive consumption (prosumption). This has resulted in commercial Internet platforms that allow user-generated content production. Surveillance of productive online consumption has brought about new forms of real-time surveillance that are at the heart of a capital accumulation model that is based on targeted advertising. At the same time, this latest development of economic surveillance is based on, connected to and mediated with older forms of surveillance.

The factory is the space for the production of economic value. Sut Jhally[54] says that in mediated audience commodification "watching is an extension of factory labour" and that the living room is therefore a factory and space of the surveillance of audience labour. The family is the social realm of housework that recreates labour power. Its main organizational unit is the household. In this respect one can say that the factory in modern society has always extended into the household.

Italian Autonomist theory has argued that the production of value has especially since the capitalist crisis in the 1970s diffused from the factory as space of the organization of wage labour into the broader realm of society. The contemporary globalization of capitalism has dispersed the walls of the wage labour factory all over the globe. Due to the circumstance that capital cannot exist without non-wage labour and exploits the commons that are created by all, society has become a factory. Different forms of unpaid and low paid work would be at the heart of what Autonomists call the social worker, who works in the social factory: "all of society lives as a function of the factory and the factory extends its exclusive domination over all of society".[55]

The commons of society are structures that are needed for all humans to exist. They are created and consumed by all humans as part of their basic life activities. They include communication, nature, welfare, health care, education, knowledge, arts and culture, food, housing. Communication is part of the commons of society. Denying

[54] Sut Jhally, *The Codes of Advertising* (New York: Routledge, 1987), 83.

[55] Mario Tronti. In: Harry Cleaver, "The Inversion of Class Perspective in Marxian Theory. From Valorisation to Self-Valorisation," in *Open Marxism. Vol. 2*, ed. Werner Bonefeld, Richard Gunn and Kosmos Psychopedis (London: Pluto, 1992), 137.

humans to communicate is like denying them to breathe fresh air; it undermines the conditions of their survival. Communication is part of basic human survival processes. In recent decades, the commons have become strongly commodified.

David Harvey describes neoliberalism as an ideology and organizational form of capitalism that is based on the principle of the commodification of everything. "Commodification presumes the existence of property rights over processes, things, and social relations, that a price can be put on them, and that they can be traded subject to legal contract. […] In practice, of course, every society sets some bounds on where commodification begins and ends".[56] Neoliberal capitalism has largely widened the boundaries of what is treated as a commodity. "The commodification of sexuality, culture, history, heritage; of nature as spectacle or as rest cure; […] – these all amount to putting a price on things that were never actually produced as commodities".[57] Antonio Negri and Michael Hardt argue that the "metropolis is a factory for the production of the common. […] With the passage to the hegemony of biopolitical production, the space of economic production and the space of the city tend to overlap. There is no longer a factory wall that divides the one from the other, and 'externalities' are no longer external to the site of production that valorizes them. Workers produce throughout the metropolis, in its every crack and crevice. In fact, production of the common is becoming nothing but the life of the city itself".[58] Nick Dyer-Witheford says that the rise of the social workers has resulted in the emergence of the "factory planet"[59] – the factory as locus for the production of value and commodities is everywhere, commodification has become universal and total. What Harvey, Negri & Hardt and Dyer-Witheford point out is that the boundaries of the factory have enlarged from the wage labour place into society and that thereby exploitation has become more global and more pervasive.

The factory is an inherent creation of capitalism. It is the space, where the exploitation of labour and the creation of value take place. The factory is not static, but develops and changes its organizational forms along with the historical trajectory of capitalism. This means that there is not one type of factory in a historical period of capitalism, but there are different types of factories that are all connected to each other and are necessary organizational forms of capital accumulation. In contemporary capitalism, we find e.g. the blue collar/white collar factories, the Internet factory, the sweatshop factory, the domestic factory (household), etc.

The rise of online playbour is situated in the context of the neoliberal commodification of the commons: the Internet is a strongly commercialized and commodified system

[56] David Harvey, *A Brief History of Neoliberalism* (Oxford: Oxford University Press, 2007), 165.

[57] ibid, 166.

[58] Michael Hardt and Antonio Negri, *Commonwealth* (Cambridge, MA: Harvard University Press, 2009), 250 f.

[59] Nick Dyer-Witheford, "Digital Labour, Species Being and the Global Worker," *Ephemera* 10 (3/4): 485.

[60] http://www.internetworldstats.com/stats.htm.

that is based on knowledge as commodity. The Internet is an almost ubiquitous factory and realm of the production of audience commodities and a space of the surveillance of playbour. Not everyone in the world has access to and is exploited on the Internet factory: as of December 31, 2011, 32.7% of the world population was online.[60] The Internet is a highly commercialized and commodified space. When we talk about broadcasting (television or radio), we have an idea of what public service broadcasting is about (although it has also largely been privatized). But in relation to the Internet, there are hardly any ideas and visions of what a public service or commons-based Internet could look like because it is so heavily controlled and in the hands of capitalists, which shows the ubiquity of exploitation and commodification on the Internet. Wikipedia is the only site under the top-100 used web platforms in the world that is not operated by a profit-oriented business. It is run by a non-profit foundation (the Wikimedia Foundation). This shows that exploitation and commodification are not total, but nearly total. Most of the online time is commodified online time, a smaller share is non-commodified.

Social media and the mobile Internet make the audience commodity ubiquitous and the factory not limited to your living room and your wage work place – the factory and work place surveillance are also in all in-between spaces. The entire planet is today a surveilled capitalist factory. Internet user commodification is part of the tendency of the commodification of everything that has resulted in the generalization of the factory and of exploitation. Neoliberal capitalism has largely widened the boundaries of what is treated as a commodity.

Internet labour and its surveillance are based on the surveillance, blood and sweat of super-exploited labour in developing countries. Alain Lipietz (1995) has in this context spoken of the emergence of "bloody Taylorism" as a contemporary accumulation regime that is coupled to two other accumulation regimes (peripheral Fordism, post-Fordism).[61] Bloody Taylorism is based on the "delocalization of certain limited Taylorist industrial activities towards social formations with very high rates of exploitation".[62] "To the traditional oppression of women, this strategy adds all the modern weapons of anti-labour repression (official unions, absence of civil rights, imprisonment and torture of opponents)".[63] Taylorism has not been replaced, we do not live in an age of post-Taylorism, rather we are experiencing an extension and intensification of Taylorism that is complemented by new ideological forms of workforce control. The emergence of workplayplaces is a tendency in contemporary capitalism that interacts with established forms of work and play. The corporate Internet requires for its existence the exploitation of the labour that exists under bloody Taylorist conditions. On top of this foundation that makes heavy use of

[61] Alain Lipietz. 1995. "The Post-Fordist World: Labour Relations, International Hierarchy and Global Ecology," *Review of International Political Economy* 4 (1): 1–41.

[62] ibid, 10.

[63] ibid, 11.

[64] Students & Scholars Against Corporate Misbehaviour (SACOM), iSlave Behind the iPhone: Foxconn Workers in Central China. http://sacom.hk/wp-content/uploads/2011/09/20110924-islave-behind-the-iphone.pdf.

traditional workplace surveillance, we find various workplayplaces on the Internet, where users work without payment and deterritorialize the boundaries between play and work.

Students & Scholars Against Corporate Misbehaviour (SACOM)[64] reported that Chinese Foxconn workers who produce iPhones, iPads, iPods, MacBooks and other ICTs are facing the withholding of wages, forced and unpaid overtime, the exposure to chemicals, harsh management, low wages, bad work safety, lack of basic facilities, etc. In 2010, 18 Foxconn employees attempted suicide, 14 of them succeeded.[65] SACOM describes Foxconn workers as "iSlave Behind the iPhone".[66] This example shows that the exploitation and surveillance of digital labour, i.e. labour that is needed for capital accumulation with the help of ICTs, is in no way limited to unpaid user labour, but includes various forms of labour – user labour, wage labour in Western companies for the creation of applications, and slave-like labour that creates hardware (and partly software) in developing countries under inhumane conditions. Surveillance of Foxconn workers is direct, coercive, disciplinary, and Taylorist. "Foxconn's stringent military-like culture is one of surveillance, obedience and not challenging authority. Workers are told obey or leave".[67] "Supervisors yell at workers with foul language. Workers experience pressure and humiliation. Workers are warned that they may be replaced by robots if they are not efficient enough. Apart from scolding by frontline supervisors, other forms of punishment include being required to write confession letters and copying the CEO's quotations. A majority of workers have to stand for 10 hours during work shifts. There is no recess as promised by Foxconn. Some workers suffer from leg cramps after work. Workers have extra workloads or have to skip the second meal break under the arrangement of 'continuous shifts'. […] At the entrance of each building, there is a worker station to check the identities of the workers".[68]

Different forms of surveillance and control are needed for controlling and exploiting digital labour. Self-control and playbour that feels like fun, but creates parts of the value, is only one part of the labour process that has its foundation in a racist mode of production and exploitation of workers in developing countries. The exploitation of play workers in the West is based on the pain, sweat, blood and death of workers in developing countries. The corporate Internet needs for its existence both playbour and toil, fun and misery, biopolitical power and disciplinary power, self-control and surveillance. The example of the Foxconn factories discussed earlier shows that the exploitation of Internet playbour needs as a precondition and is coupled to the bloody Taylorist exploitation of workers in the developing world.

The factory is not only the space of surveillance, but also a space for potential or actual resistance. To overcome the old and new forms of workplace surveillance that are tightly coupled to each other and form parts of a global capitalist factory, social

[65] http://en.wikipedia.org/wiki/Foxconn_suicides, accessed on February 8, 2011.

[66] ibid.

[67] CNN Online, Apple Manufacturing Plant Workers Complain of Long Hours, Militant Culture. http://edition.cnn.com/2012/02/06/world/asia/china-apple-foxconn-worker/index.html.

[68] SACOM, op cit.

struggles are needed. Ongoing struggles in the context of the crisis of capitalism are attempts to resist the commodification of everything. Resisting the commodification and surveillance of the communication commons requires realizing that the creation of an alternative Internet is in need of struggles for a society that transcends the universe of exploitation and commodification. These are struggles for the appropriation of the commons.

References

Arendt, Hannah. 1958. *The human condition*, 2nd ed. Chicago: University of Chicago Press.
Boltanski, Luc, and Eve Chiapello. 2007. *The new spirit of capitalism*. London: Verso.
Braverman, Harry. 1974. *Labor and monopoly capital*. New York: Monthly Review Press.
Clark, Leigh A., and Sherry J. Roberts. 2010. Employer's use of social networking sites: A socially irresponsible practice. *Journal of Business Ethics* 95(4): 507–525.
Cleaver, Harry. 1992. The inversion of class perspective in Marxian theory. From valorisation to self-valorisation. In *Open marxism*, vol. 2, ed. Werner Bonefeld, Richard Gunn, and Kosmos Psychopedis, 106–144. London: Pluto.
Davison, Kristl H., Catherine Maraist, and Mark N. Bing. 2011. Friend or foe? The promise and pitfalls of using social networking sites for HR decisions. *Journal of Business and Psychology* 26(2): 153–159.
Davison, Kristl H., Catherine Maraist, R.H. Hamilton, and Mark N. Bing. 2012. To screen or not to screen? Using the internet for selection decisions. *Employee Responsibilities and Rights Journal* 24(1): 1–21.
Deleuze, Gilles. 1995. Postscript on the societies of control. In *Negotiations*, 177–82. New York: Columbia University Press.
Dyer-Witheford, Nick. 2010. Digital labour, species being and the global worker. *Ephemera* 10(3/4): 484–503.
Engels, Friedrich. 1892/2010. *The condition of the working class in England in 1844*. Cambridge: Cambridge University Press.
Ferguson, Marjorie, and Peter Golding (eds.). 1997. *Cultural studies in question*. London: Sage.
Foucault, Michel. 2007. *Security, territory, population. Lectures at the Collège de France 1977–1978*. Basingstoke: Palgrave Macmillan.
Freud, Sigmund. 1961. *Beyond the pleasure principle*. New York: Norton.
Fuchs, Christian. 2008. *Internet and society. Social theory in the information age*. New York: Routledge.
Fuchs, Christian. 2010a. Labor in informational capitalism and on the internet. *The Information Society* 26(3): 179–196.
Fuchs, Christian. 2010b. Social software and web 2.0: Their sociological foundations and implications. In *Handbook of research on Web 2.0, 3.0, and X.0: Technologies, business, and social applications*, vol. II, ed. San Murugesan, 764–789. Hershey: IGI-Global.
Fuchs, Christian. 2012a. A contribution to the critique of the political economy of Google. *Fast Capitalism* 8(1). http://www.uta.edu/huma/agger/fastcapitalism/8_1/fuchs8_1.html.
Fuchs, Christian. 2012b. Political economy and surveillance theory. *Critical Sociology* 38, 2 April 2012. doi 10.1177/0896920511435710
Garnham, Nicholas. 1995/1998. Political economy and cultural studies: Reconciliation or divorce? In *Cultural theory and popular culture*, ed. John Storey, 600–612. Harlow: Pearson.
Grossberg, Lawrence. 1995/1998. Cultural studies vs. Political economy. Is anybody else bored with this debate? In *Cultural theory and popular culture*, ed. John Storey, 613–624. Harlow: Pearson.
Habermas, Jürgen. 1987. *The theory of communicative action*, Lifeworld and system: A critique of functionalist reason, vol. 2. Boston: Beacon.

Habermas, Jürgen. 1989. *The structural transformation of the public sphere*. Cambridge, MA: MIT Press.
Hardt, Michael, and Antonio Negri. 2000. *Empire*. Cambridge, MA: Harvard University Press.
Hardt, Michael, and Antonio Negri. 2009. *Commonwealth*. Cambridge, MA: Harvard University Press.
Harvey, David. 2007. *A brief history of neoliberalism*. Oxford: Oxford University Press.
Jhally, Sut. 1987. *The codes of advertising*. New York: Routledge.
Jhally, Sut, and Bill Livant. 1986. Watching as working. The valorization of audience consciousness. In *The spectacle of accumulation. Essays in culture, media, & politics*, ed. Sut Jhally, 24–43. New York: Peter Lang.
Kücklich, Julian. 2005. Precarious playbour. *Fibreculture Journal* 5. http://five.fibreculturejournal.org/fcj-025-precarious-playbour-modders-and-the-digital-games-industry/.
Lipietz, Alain. 1995. The post-fordist world: Labour relations, international hierarchy and global ecology. *Review of International Political Economy* 4(1): 1–41.
Marcuse, Herbert. 1955. *Eros and civilization*. Boston: Beacon.
Marx, Karl. 1867. *Capital*, vol. I. London: Penguin.
Parker, Mike, and Jane Slaughter. 1995. Unions and management by stress. In *Lean work: Empowerment and exploitation in the global auto industry*, ed. Steven Babson, 41–53. Detroit: Wayne State University Press.
Robins, Kevin, and Frank Webster. 1999. *Times of technoculture: From the information society to the virtual life*. London: Routledge.
Sánchez Abril, Patricia, Avner Levin, and Alissa Del Riego. 2012. Blurred boundaries social media privacy and the twenty-first-century employee. *American Business Law Journal* 49(1): 63–124.
Smythe, Dallas W. 1977. Communications: Blindspot of western Marxism. *Canadian Journal of Political and Social Theory* 1(3): 1–27.
Smythe, Dallas W. 1981. *Dependency road*. Norwood: Ablex.
Taylor, Fredrick W. 1911. *The principles of scientific management*. New York: Harper.
Trottier, Daniel. 2012. *Social media as surveillance*. Farnham: Ashgate.

Chapter 3
From Market-Making Tool to Fundamental Right: The Role of the Court of Justice in Data Protection's Identity Crisis

Orla Lynskey

3.1 Introduction

The European Data Protection Directive, Directive 95/46 EC,[1] entered in force in 1995. It was the first instrument of its kind in the then European Community (EC), now European Union (EU), and has served as a blueprint for data protection regimes subsequently established across the globe. As such, it is a rare example of EU regulatory supremacy. Directive 95/46 EC (the Directive) pursues dual objectives; it facilitates the establishment of the internal market and protects fundamental rights in the EU. The Directive could therefore be said to have a "split personality". Its precise nature is difficult to discern; is it a tool for market integration? Or is it an instrument for the protection of fundamental rights? The Court of Justice has struggled with these questions of identity,[2] initially downplaying the Directive's fundamental rights persuasions. However, in recent years, particularly following the entry into force of the Treaty of Lisbon, the Court has placed increasing emphasis on the Directive's rights-based characteristics, sometimes (inadvertently) to the detriment of its market-making objective.

[1] European Parliament and Council Directive 95/46/EC of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L281/23.

[2] The Court has been asked to balance internal market objectives with conflicting fundamental rights objectives on a number of occasions in recent years. See, for instance, C-112/00 *Eugen Schmidberger Internationale Transporte und Planzüge v Republic of Austria* [2003] ECR I-5659, C-36/02 *Omega Spielhallen-und Automatenaufstellungs-GmbH v Oberbürgermeisterin der Bundesstadt Bonn* [2004] ECR I-9609 and the Viking and Laval cases (C-438/05 *International Transport Workers' Union v Viking Line* [2007] ECR I-10779 and C-431/05 *Laval un Partneri Ltd v Svenska Byggnadsarbetareförbundet* [2007] ECR I-11767).

O. Lynskey (✉)
Lucy Cavendish College, Cambridge University, Lady Margaret Road,
Cambridge, CB3 0BU, England, UK
e-mail: ol226@cam.ac.uk; lynskeyo@gmail.com

S. Gutwirth et al. (eds.), *European Data Protection: Coming of Age*,
DOI 10.1007/978-94-007-5170-5_3,

The aim of this paper is consider the relationship between these two potentially contradictory objectives. It seeks to demonstrate two main points. Firstly, that the ambiguity regarding the relationship between the Directive's dual objectives could lead to doubts concerning its validity. Secondly, while the Directive's market-making characteristics have been interpreted loosely by the Court, there are strong indications that in the post-Lisbon Treaty era its fundamental rights dimension will become even more prominent in the Court's case law. This paper will therefore be structured as follows. Firstly, in Sect. 3.2, data protection's 'market-making' vocation will be critically considered. The Directive was enacted on the basis of Article 100a of the EC Treaty (then Article 95 EC, now Article 114 TFEU) which allows the EU to enact legislation to improve the functioning of the internal market. The use of this provision as the Directive's legal basis will be discussed and placed in its historical context. Then, in Sect. 3.3, by referring to the jurisprudence of the Court of Justice, it will be demonstrated that data protection legislation has been applied in a manner that loosened the link with its original market harmonisation aim. In Sect. 3.4, it will be shown that data protection's fundamental rights objectives have now taken centre stage in the Court of Justice's case law and that less attention is now paid to its market harmonisation goals. In Sect. 3.5 the importance of clarifying the objectives of data protection will be emphasised and some concluding remarks will be made.

3.2 A Critical Analysis of the 'Market-Making' Vocation of European Data Protection Law

In this section, the role of data protection as a tool for market integration will be analysed. The Directive has dual objectives; ensuring the free flow of personal data in the EU and protecting the fundamental rights and freedoms of natural persons whose personal data are processed. The dynamic between these two objectives will be examined through a historical lens (by considering the evolution of data protection in the EU legal order) in order to shed some light on their respective roles (Sect. 3.2.1). Then, the choice of Article 114 TFEU as a legal basis for the Directive will be considered in light of the relevant case law of the Court of Justice (Sect. 3.2.2). It will be seen that the choice of legal basis for the Directive, which effectively ignores its fundamental rights objectives, is, at best, controversial.

3.2.1 The Emergence of the Dual Objectives of European Data Protection Law

The Data Protection Directive is adopted on the basis of what is now Article 114(1) TFEU. According to this provision, the legislature may adopt measures to approximate national law, regulation or administrative action provided these measures have 'the

establishment and functioning of the internal market' as their objective. According to the explanatory memorandum to the Data Protection Directive[3] the free flow of data between Member States, which the proposed legislation would enable, is apparent at three levels. First, the Treaty's fundamental freedoms require that personal data is transferable between business people involved in cross-border activities. Second, the abolition of frontiers within the internal market necessitates the free flow of data as it requires cooperation between national authorities. Third, data exchange is necessary for scientific purposes.[4] Rather than explicitly permitting the free flow of data for these purposes, the Directive instead sought to eliminate disparities between the laws of the Member States by introducing a uniform regulatory environment.

Attempts to approximate national laws in this field had been ongoing for years; the OECD issued Guidelines[5] in September 1980 with the aim of ensuring the development of national data protection laws in a manner that would not lead to disruptions of cross-border data flows,[6] and consequently international trade.[7] However, the non-binding nature of these Guidelines limited their effectiveness in achieving this aim and divergences between national laws persisted. The European Commission also attempted to limit these divergences to an acceptable level by encouraging compliance by EU Member States with the Council of Europe's Convention No.108,[8] which set out many of the rights, obligations and safeguards that are still visible in the EU's current regime.[9] The Commission issued a recommendation that Member States ratify Convention No.108 before the end of 1982, reserving the right to propose legislation itself if this did not occur.[10] However, this indirect attempt to harmonise national laws by the European Commission was not successful; by the

[3] European Commission, Communication on the protection of individuals in relation to the processing of personal data in the Community and Information Security COM (90) 314 final.

[4] Ibid, 16.

[5] OECD, "Guidelines Governing the Protection of Privacy and the Transborder Flows of Personal Data", 23 September 1980. (Accessed on 25 May 2011, available via http://www.oecd.org/document/20/0,3746,en_2649_34255_15589524_1_1_1_1,00.html).

[6] The Guidelines set out the following (overlapping) objectives: (i) to achieve the acceptance of certain minimum standards of protection of personal data privacy; (ii) to reduce the differences between relevant domestic rules and practices in Member States; (iii) to avoid undue interference with flows of personal data between Member countries; and, (iv) to eliminate, to the extent possible, reasons which might induce Member States to restrict transborder data flows. Ibid, explanatory memorandum, §25.

[7] David Bainbridge, *Data Protection*, 2nd ed., xpl publishing, 2005, 16.

[8] Council of Europe, *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data,* ETS No.108, 28.I.1981, (www.conventions.coe.int/Treaty/EN/Treaties/Html/108.htm, accessed on 15 April 2010).

[9] Convention No.108 imposed obligations on those who processed personal data, set out a catalogue of rights for individuals and emphasised that certain categories of data should not be processed unless subject to appropriate safeguards provided for by law.

[10] European Commission, Recommendation of 29 July 1981 relating to the Council of Europe Convention for the protection of individuals with regard to automatic processing of personal data [1981] OJ L246/31.

end of 1989 only seven Member States had ratified Convention No.108[11] and the legislation in place in those seven Member States diverged significantly.[12] Despite the Commission's preference for the organic development of homogeneous national data protection legislation,[13] its hand was therefore forced to take direct action to approximate national laws. It adopted a proposal for the Data Protection Directive as part of a package of suggested legislative measures[14] in 1990. The divergences between the data protection legislation (or lack thereof) in place in the Member States was therefore clearly a significant factor in the Commission's decision to propose legislation on the matter. These divergences were preventing, or at least rendering more difficult, the free flow of data across borders required for business and research, and to dismantle borders in the EU. It was therefore only by ensuring that each Member State offered a uniform level of protection of fundamental rights in the context of personal data processing that the EU could achieve this internal market aim. Viewed from this angle, the proposed legislation was intended to improve the functioning of the internal market and fell squarely within the EU's sphere of competences under the then Article 100a EC.

Independently of this internal market aim, from the early 1970s the European Institutions demonstrated their concern that citizens' rights be protected in the context of data processing. Although the European Commission was conscious of

[11] Council of Europe, Chart of signatures and ratifications (accessed on 18 July 2011 via http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=108&CM=&DF=&CL=ENG). The countries which had ratified the Convention were Denmark, France, Germany, Luxembourg, the Netherlands, Spain and the UK while Belgium, Greece, Ireland, Italy and Portugal had not yet. Ireland ratified the Convention in 1990 and already had data protection legislation in place before then whereas Spain did not have data protection although it had ratified the Convention.

[12] The Commission highlights that Member States differ with regard to: "the covering of manual data files, the protection of legal persons, the procedures prior to the creation of files, the extent of the obligation to notify, the provision of information at the time of collection of data, the processing of sensitive data and transfer to other countries". See Commission Communication on protection of individuals, *o.c.*, 15.

[13] When the European Commission addressed a Communication to the Council in 1973 setting out a strategy for the competitive development of the Community's nascent data-processing industry, it noted that "common measures for the protection of the citizen would be needed". The Commission's aim at this point was however to immediately establish "common ground rules" based on "genuine political consensus" in order to avoid being obliged to harmonise conflicting national legislation at a later stage. See European Commission, Communication to the Council on a Community Data-Processing Policy SEC (73) 4300 final, 13 (§39).

[14] This package included the following measures: Proposal for a Council Decision in the field of Information Security OJ C 277/18; Proposal for a Council Directive concerning the protection of personal data and privacy in the context of public digital telecommunications networks, in particular the integrated services digital network (ISDN) and public digital mobile networks OJ C 277/12; Proposal for a Council Directive concerning the protection of individuals in relation to the processing of personal data OJ C 277/3; Recommendation for a Council Decision on the opening of negotiations with a view to accession of the European Communities to the Council of Europe Convention for the Protection of Individuals with regard to the automatic processing of personal data; Commission Communication on the protection of individuals in relation to the processing of personal data in the Community and Information Security. (Accessed on 14 July 2011, available via http://aei.pitt.edu/3768/1/000273_1.pdf)

the need to protect the rights of citizens whose data would be processed by the data-processing industry it sought to foster, as mentioned above the Commission initially wished to leave the protection of these rights to Member States. The European Parliament felt otherwise; in May 1975 it adopted a resolution calling for legislation to protect the rights of individuals in the context of data processing.[15] The Commission then subsequently proposed that a study be conducted to supplement the work of the European Parliament, and to "provide basic data in the Community for a political debate to establish guidelines for legislation and practices regarding security and the protection of citizens' rights".[16] When the abovementioned legislative package was eventually proposed in 1990, the explanatory memorandum identified three main problems with the approach in place in Member States. The first of these was that the lack of specific national laws or their deficiencies did "not reflect the Community's commitment to the protection of fundamental rights".[17] Consequently, it is clear that securing a high level of fundamental rights protection constituted an independent objective of the Directive from the outset.

Given the Directive's dual vocations, to ensure the functioning of the internal market and to protect fundamental rights, it could be questioned whether the EU legislature's choice of Article 100a EC as the sole legal basis for the Directive was appropriate. It is not disputed that one of the objectives the Directive sought to achieve was market harmonisation. For instance, the title of the 1990 draft of the Directive,[18] which omitted any reference to the free movement of data, was amended by Council with the explicit intention of emphasizing that the proposal aims to establish a "working single market". [19] This is one of many examples which illustrates that the Directive's economic, market harmonisation aspect was never overlooked by the European legislature. What the preceding section sought to highlight was that this was not the Directive's sole objective; independently of this genuine objective to establish the free movement of data and to improve the functioning of the internal market, the Directive also sought to secure a high level of fundamental rights protection in the rapidly emerging field of data processing. It is therefore advocated, as will be outlined in Sect. 3.2.2, that neither of these objectives is "secondary" to the other and, consequently the use of Article 100a alone as a legal basis was potentially invalid.

[15] European Parliament, Resolution on the Protection of the Rights of the Individual in the Face of Developing Technical Progress in the Field of Automatic Data Processing [1975] OJ C60/48.

[16] European Commission, 'Community Policy for Data Processing' COM 75 (467) final, 47/48, §2.3.

[17] Commission Communication on protection of individuals, *o.c.*, 15.

[18] Proposal for a Council Directive concerning the protection of individuals in relation to the processing of personal data, *o.c.*

[19] Amended proposal for a Council Directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data, COM (92) 422 final, 8. (Accessed via http://aei.pitt.edu/10375/ on 13 April 2012).

3.2.2 The Competence Question: The Legitimacy of EU Legislation in the Human Rights Sphere

A considerable body of Court of Justice case law exists on the use of Article 100a EC (now Article 114 TFEU) as a legal basis. These cases share a common theme; Member States challenge the validity of EU legislation which relies on this Article as its legal basis arguing that the EU lacks the competence to legislate in the relevant field. It clearly follows from the previous section of this paper that the Data Protection Directive has two distinct, yet interlinked, goals; to approximate national laws with the object of establishing the internal market and to protect fundamental rights in the context of data processing. In order to achieve the first goal, the second goal must be achieved. Given this unusual relationship between the two objectives, should the Directive have been enacted on dual legal bases?

The Court has previously had the opportunity to consider the use of dual legal bases by the legislature. It has held that if a legislative act has a twofold purpose and if one of these is identifiable as the predominant purpose, with the other being merely incidental, the act must be founded on a sole legal basis, the one required by the predominant purpose.[20] The question is therefore whether the protection of fundamental rights could be viewed as "merely incidental" to the internal market ambitions of the Data Protection Directive. Given the legislative history outlined above, in particular the strong support by the European Parliament for legislation in this area irrespective of internal market concerns, it would be disingenuous to argue that the protection of fundamental rights was an incidental consideration when the Directive was adopted. Rather, the Directive arguably pursues two "indissociably linked objectives, with none being secondary or indirect in relation to the other". In such a situation, according to the case law of the Court, such a legislative act may, exceptionally, be founded on the various corresponding legal bases.[21]

Why therefore does the Data Protection Directive not specify a second legal basis to justify its legislative action in the human rights sphere? One answer is that, as the Court pointed out in *Opinion 2/94*,[22] "no Treaty provision confers on the Community institutions any general power to enact rules on human rights".[23] However, by the time the Directive was adopted the Court of Justice had woven human rights considerations into its jurisprudence and, in an initial tranche of judgments, spurred on by the Constitutional Courts of the Member States, it guaranteed that individual rights would be protected against acts of the institutions. Indeed,

[20] C-491/01 *Queen v. Secretary of State for Health, ex parte British American Tobaco (Inv) Ltd & Imperial Tobacco Ltd.* 2002 ECR I-11453, §94.

[21] *Opinion 2/00* [2001] ECR I-9713, §23. See also, C-300/89 *Commission v Council (Titanium Dioxide)* [1991] ECR I-2867, §13 & 17.

[22] *Opinion 2/94* [1996] ECR I-1759.

[23] Ibid, §27.

cases such as *Internationale Handelsgessellshaft*[24] and *Nold*[25] were delivered almost contemporaneously to the European Parliament's resolution on the protection of individual rights in personal data processing. In subsequent waves of case law the Court of Justice expanded on the scope of human rights protection offered by EU law when it held that individual fundamental rights were protected when Member States implemented EU law[26] or derogated from EU law.[27]

Despite the Court of Justice's significant role in bolstering the level of fundamental rights protection offered by the EU, it is advocated that such protection did not extend so far as to justify the EU legislating on what was essentially a fundamental rights matter. EU competences are governed by the principle of conferral, according to which any competence which has not been expressly conferred upon the Union by the Treaties continues to fall within the sphere of competence of the Member States. Therefore, a distinction should be drawn between the obligation on the EU institutions to ensure the observance of the respect for fundamental rights in its actions (which can also be viewed as a negative duty not to breach fundamental rights when it acts) and recognising the competence of the EU to legislate in order to further the protection of fundamental rights. The Data Protection Directive clearly falls into the latter category. This has prompted authors such as Rule and Greenleaf to note that the Data Protection Directive is "the first EU Directive to expressly accord fundamental rights a prominent place".[28] The Directive certainly stretches the lawful limits of EU action. Moreover, as will be seen in the following section, the Court of Justice has overlooked opportunities to consider whether the EU was acting *ultra vires* when it enacted the Data Protection Directive. Moreover, the Court's jurisprudence has loosened the link between the Directive and its market harmonisation aims, thereby casting further doubts on its validity.

3.3 Loosening the Links Between Data Protection and Market Harmonisation?

In this section it will be argued that the Court of Justice's interpretation of the Directive has had the effect of loosening the Directive's links with its stated market harmonisation objective. This has occurred because the Court's case law has interpreted the Directive's scope of application as widely as possible (Sect. 3.3.1) and left a broad margin of discretion to national authorities when implementing the Directive (Sect. 3.3.2).

[24] C-11/70 *Internationale Handelsgessellshaft* [1970] ECR 1125.

[25] C-4/73 *Nold* [1974] ECR 491.

[26] See, for instance, C-5/88 *Wachauf* [1989] ECR I-2609.

[27] See, for instance, C-60/00 *Carpenter* [2002] ECR I-6279.

[28] Rule and Greenleaf, *Global Privacy Protection: The First Generation*, Edward Elgar Publishing, 2008, 31.

3.3.1 The Broad Conception of the Directive's Scope of Application

In the first case to come before the Court of Justice in the field of data protection, *Österreichischer Rundfunk*,[29] the national referring court asked the Court to consider whether a requirement in Austrian legislation that the salaries of senior public officials be communicated to the national audit body, transmitted to the national Parliament and later made publicly available, was compatible with Directive 95/46 EC. The applicability of the Directive to the facts of the case was disputed before the Court as there were strong indications the situation was a "wholly internal" one[30] that did not have the requisite inter-State element to fall within the material scope of Community law.

Those whose data had been processed in accordance with the national law argued that the auditing activity fell within the scope of Community law because it would negatively affect their possibility to seek employment in other Member States (by limiting their chances to negotiate salaries with foreign companies) and it would deter nationals of other Member States from seeking employment with the audited bodies in Austria.[31] An audited commercial airline also argued that the processing activity would make it more difficult for it to hire employees thereby putting it at a competitive disadvantage and interfering with the free movement of workers.[32] The auditing body and the Austrian and Italian governments[33] argued that the control activity pursued public interest objectives in the field of public accounts and was therefore not subject to EU law. Moreover, they advocated that any potential deterrent effect on the free movement of workers was too 'uncertain and indirect' to allow a link to be made with Community law. Advocate General Tizzano agreed, highlighting that the possible effect on the free movement of workers was strained and unconvincing.[34] The Court's case law had previously stated that a purely hypothetical prospect of employment in another Member State is insufficient to establish the Community law element required by the Treaty's free movement provisions.

---

[29] C-139/01 *Österreichischer Rundfunk and Others* [2003] ECR I-4989.

[30] This is the terminology used by the Court when refusing to apply the Treaty's free movement provisions to situations which are "wholly internal to a Member State"; an inter-state element must be demonstrated in order to fall within the material scope of the Treaty's Internal Market provisions. See further, Barnard, *The Substantive Law of the European Union*, 2nd ed., Oxford University Press, 2010, 614.

[31] *Rundfunk*, *o.c.*, §33.

[32] *Rundfunk*, *o.c.*, §34.

[33] The European Commission agreed to a certain extent; at the hearing the Commission distinguished between the initial collection of data by the controlled bodies and the other data processing activities required by the Austrian legislation. It argued that only the initial collection, which facilitates the payment of remuneration, constituted an activity covered by EU law.

[34] Opinion of Advocate Generak Tizzano delivered on 14 November 2002 in C-139/01 *Österreichischer Rundfunk and Others*, §46.

The parties to the proceedings therefore clearly considered it necessary to establish an inter-State element to the national proceedings in order to engage a Directive based on Article 100a; the Court did not. It held that recourse to Article 100a as a legal basis does not presuppose the existence of an actual link with the free movement between Member States in every situation.[35] It drew on its previous case law on Article 100a EC to hold that what matters when justifying recourse to this legal basis is that the measure adopted "must actually be intended to improve the conditions for the establishment and functioning of the internal market".[36]

One could argue that from a practical perspective the Court's conclusion that no actual link with inter-State free movement is required is sensible; as the Court itself noted, to find otherwise would make the limits of the field of application of the Directive unsure and uncertain and would, in this way, detract from its harmonising objective.[37] On the other hand however, the Court did not consider whether the Directive *was* actually intended to improve the conditions for the establishment and functioning of the internal market. Instead, it merely noted that in "…the present case, that fundamental attribute was never in dispute before the Court…".[38] While this could be perceived as a subtle hint by the Court to future litigants to raise the issue directly before it, the Court's acceptance that the Directive pursued internal market objectives without further consideration can be criticised on both procedural and substantive grounds. Procedurally, the Court of Justice can, of its own initiative, examine whether a disputed EU act is invalid on grounds other than those stated by the national court in the order for reference.[39] Substantively, as Classen argues, the dispute about "the closeness of the case to the fundamental freedoms" related to considerations of the necessary relationship with the internal market (i.e. whether the Directive was intended to improve the conditions for the establishment and the functioning of the internal market).[40]

Moreover, the Advocate General warned the Court against finding that "processing carried out in the course of activities entirely unrelated to the establishment and functioning of the internal market" is within the Directive's scope. Nevertheless the Court's judgment mandated such an "incongruous result". The Advocate General clearly considered that the Court could only make such a finding if the protection of fundamental rights constituted an independent objective of the Directive. He noted that while the safeguarding of fundamental rights was an "important value", it was "not an *independent* objective of the Directive"[41] and emphasised that any finding to the contrary would run the risk of compromising the Directive's validity because

[35] *Rundfunk, o.c.*, §41.

[36] *Rundfunk, o.c.*, §42.

[37] Ibid.

[38] *Rundfunk, o.c.*, §41.

[39] See Broberg and Fenger, *Preliminary References to the European Court of Justice*, Oxford University Press, 2010, 418. However, it tends to raise ex officio issues more frequently in references concerning the validity of a Union act.

[40] Classen, 'C-139/01 *Österreichischer Rundfunk and Others*: case- note', (2004) 41(5) *Common Market Law Review* 1377, 1381.

[41] Opinion of Advocate General Tizzano, *o.c.*, §53.

"its legal basis would clearly be inappropriate". The Court's failure to consider this issue is all the more conspicuous as a result of this statement. One must therefore agree with Classen who suggests that the Court's silence could be regarded as a sign that "the Court was at least not sure how it would have answered if it had been asked about the validity of the Directive as such".[42]

History was to repeat itself just a few months later when questions regarding the Directive's validity were raised before the Court of Justice in *Lindqvist*.[43] Once again, Advocate General Tizzano argued that the processing in question fell outside the scope of EU law and that a finding to the contrary would mean that the legislature did not have the competence to enact the Directive. However, once again, the Court did not consider the issue. The facts of the case were as follows. Mrs. Lindqvist worked as a voluntary catechist for a church in Sweden. Of her own initiative she set up a website to introduce 18 of her colleagues to the parish. She identified her colleagues, outlined their family situation, described their activities, provided their phone numbers and also mentioned that one colleague was working part-time due to injury. Mrs. Lindqvist removed the web pages following a number of objections from her colleagues. She was nevertheless prosecuted by the Swedish authorities for processing personal data without prior notification, transferring personal data to third countries and processing sensitive data.

The Swedish court referred a number of questions to the Court of Justice, including whether the processing concerned was within the scope of Community law. The parties to the proceedings once again considered that it was a precondition for the application of the Directive that the processing in question fell within the material scope of Community law. In particular, they sought to demonstrate that the requisite "economic" element was present.[44] Mrs. Lindqvist therefore argued that the Directive only covered personal data processing in the course of an economic activity; the processing she undertook was free of charge. She advocated that should the Court find otherwise the validity of the Directive would be in question as its legal basis 'does not allow activities that have no connection with the objective of completing the internal market to be regulated at European level'.[45] The Commission attempted to identify an alternative economic link; it argued that Mrs. Lindqvist fell within the freedom of services provisions when she availed of telecommunications services in order to connect to the Internet.[46] The Advocate

[42] Classen, *o.c.*, 1381.

[43] C-101/01 *Bodil Lindqvist* [2003] ECR I- 12971.

[44] The Treaty's free movement provisions apply to economic activities. For instance, "goods" must be capable of forming the subject of "commercial transactions" (C-7/68 *Commission v. Italy (the art treasures case)* [1968] ECR 423) while "workers" must receive remuneration (C-66/85 *Lawrie-Blum v. Land Baden-Württemberg* [1986] ECR 2121).

[45] *Lindqvist*,*l.c.*, §30. Indeed, Mrs. Lindqvist argued that she was merely exercising her right to freedom of expression by creating internet pages as a leisure activity; an argument not dealt with by the Court.

[46] Opinion of Advocate General Tizzano delivered on 19 September 2002 in C-101/01 *Bodil Lindqvist*, §32.

General agreed with Mrs. Linqvist that the processing activity fell outside the scope of Community law[47] as it did not have the requisite economic element to link it to the exercise of fundamental freedoms.[48] He noted that the webpage was created 'without any intention of economic gain, solely as an ancillary activity to her voluntary work as a catechist in the parish community and outside the remit of any employment relationship'.

The European Commission also argued, in the alternative, that Community law is not confined to regulating economic activities; the Union must respect fundamental rights as general principles of EU law pursuant to Article 6 TEU.[49] However, the Advocate General once again pointed out that these fundamental rights could not constitute independent objectives of the Directive, reiterating that if the Directive were held to have other independent objectives aside from the establishment of the internal market its legal basis would be invalid.[50]

The Court recalled its finding in *Rundunk* that recourse to Article 100a as legal basis does not presuppose the existence of an actual link with free movement between Member States in every situation.[51] It held that it would "not be appropriate" against that background to consider on a case by case basis whether the specific activity at issue affected freedom of movement between Member States.[52] . Article 3 of the Directive excludes from its scope personal data processing "in the course of an activity which falls outside the scope of Community law". In order to bolster its conclusion that the processing concerned fell within the scope of Community law, the Court noted that the examples of activities "falling outside the scope of Community law" mentioned in Article 3(2) are activities of the State or State authorities, unrelated to the fields of activity of individuals.[53] It deduced from this that the exception only applied to activities which could be classified in the same category[54] and that charitable or religious activities such as those carried out by Mrs. Lindqvist were not within this category.[55] Again, the Court's reasoning on this point is flawed. It is submitted that the Article 3(2) exception sought to distinguish between first pillar ("Community law") processing activities and second and third pillar ("EU law") processing activities. Indeed, the examples in Article 3(2) confirm

[47] Ibid, §35.

[48] Ibid, §36.

[49] Bizarrely, the Commission also argued that the Directive was intended to 'contribute to the social progress and well-being of the individual and that it cannot be ruled out that it is intended to regulate the free movement of personal data within as a social activity in the internal market'.

[50] Ibid, §42.

[51] *Lindqvist*, *o.c.*, §40.

[52] Ibid, §42.

[53] Ibid, §43.

[54] Ibid, §44.

[55] Ibid, §45.

this point.[56] This Article should therefore not have been relied on by the Court to support its distinction between activities which fall within the scope of Community law and those which remain within the scope of national law.

It therefore follows from this section that the effect of both the *Lindqvist* and the *Rundunk* judgments is to distance the application of the Data Protection Directive from the traditional realms of application of Community law and loosens its link with the internal market.

3.3.2 The Margin of Discretion Left to National Authorities

In this section, it will be demonstrated that the Court has interpreted the Directive in such a way as to leave a large margin of discretion to national authorities, thereby jeopardising its market harmonisation aim.

In the *Satamedia*[57] case, Satakunnan collected personal data from the Finish tax authorities relating to persons who earned over a certain threshold. Abstracts from the information collected, which included the names, earnings to the nearest €100 and wealth tax levied on the 1.2 million people concerned, were then published in local editions of a national newspaper. Satakunnan then transferred this information on CD-ROM discs to Satamedia who disseminated it via text message. The Finnish Data Protection Authority's refusal to prevent Satamedia from providing this messaging service was challenged before the national courts and culminated in a preliminary reference to the Court of Justice.

The Court highlighted that the Directive's objective (to provide for the free flow of personal data whilst protecting fundamental rights)[58] must be reconciled with the right to freedom of expression. It found that Article 9 of the Directive, which provides for derogations to the Directive when data is processed for "journalistic purposes" or for "the purpose of artistic or literary expression", provides the means to do this. The Court concluded that the activities in question could constitute "journalistic activities" if "their object is the disclosure to the public of information, opinions or ideas, irrespective of the medium which is used to transmit

[56] Examples of such activities are provided in the Directive; activities set out in Chapter V and VI TEU (relating to CFSP and Police and Judicial Cooperation respectively) and activities concerning public security, defence, State security and the activities of the State in areas of criminal law. As a result of this provision, even after the entry into force of the Lisbon Treaty and the collapse of the pillar structure, the Directive does not automatically apply to former third pillar matters. See further, Hijmans and Scirocco, "Shortcomings in EU Data Protection in the Third and Second Pillars. Can the Lisbon Treaty be expected to help?" (2009) 46(5) *Common Market Law Review* 1485, 1515.

[57] C-73/07 *Tietosuojavaltuutettu* v. *Satakunnan Markkinapörssi OY, Satamedia* [2008] ECR I-09831.

[58] Ibid, §52.

them".[59] It was for the national court to consider this on the facts. What is noteworthy about the Court's finding is that it will allow national courts to exempt virtually any form of expression involving personal data processing from the scope of the Directive. Indeed, Oliver notes that "the Court's open-ended ruling appears to allow national courts virtually unfettered discretion in defining the concept of journalism".[60] The Court's judgment is therefore guaranteed to diversify, rather than harmonise, national laws. This is all the more shocking given that such a broad interpretation sits uneasily with the jurisprudence on Article 10 of the European Convention of Human Rights (ECHR)[61] which includes within its scope only expression that is in the public interest.[62]

In *Promusicae*[63] the Court was asked to consider whether EU law precludes Member States from adopting national legislation that obliges internet service providers (ISPs) to provide the personal data of alleged copyright infringers to copyright holders in order to facilitate civil proceedings. Although it was primarily the E-Privacy Directive[64] at issue in that case, and not the Data Protection Directive, the E-Privacy Directive was also enacted on the basis of Article 95 EC therefore it is illustrative of the extent to which the Court takes market harmonisation into consideration in applying European data protection law. Promusicae, an association of music producers and publishers, lodged an application before a Spanish court against Telefónica, an ISP, requesting that Telefónica disclose the names and addresses of a number of its clients. Promusicae had data to indicate that acts of copyright infringement had been committed from certain IP addresses however it needed the names and addresses of the IP address holders in order to commence civil proceedings. The E-Privacy Directive ensures the confidentiality of electronic communications on public networks. However, Article 15(1) allows Member States to impose restrictions on the Directive's general confidentiality obligation when they "constitute a necessary, appropriate and proportionate measure within a democratic society to safeguard national security (i.e. State security), defence, public

[59] In her Opinion Advocate General Kokott proposed that the term "journalistic purposes" be restrictively construed. She suggested that information that is disseminated for the purposes of informing public debate, as opposed to information that is published for the "sole purpose of satisfying the curiosity of a particular readership", should fall within the scope of this term. Opinion of Advocate General Kokott delivered on 8 May 2008 in C-73/07 *Tietosuojavaltuutettu* v. *Satakunnan Markkinapörssi OY, Satamedia*, §69–§74.

[60] Oliver, "The protection of privacy in the economic sphere before the European Court of Justice" (2009) 46(5) *Common Market Law Review* 1443, 1463.

[61] Council of Europe, *Convention for the Protection of Human Rights and Fundamental Freedoms*, ETS No. 5, 4.XI.1950, www.conventions.coe.int/treaty/en/treaties/html/005.htm.

[62] Ibid.

[63] C-275/06 *Productores de Música de España (Promusicae) v. Telefónica de España* [2008] ECR I-271.

[64] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) [2002] OJ L201/37.

security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communication system, as referred to in Article 13(1) of Directive 95/46/EC".

The Court held that this provision concerned the prosecution of criminal activities or activities of the State unrelated to the field of activity of individuals; therefore, it did not include the bringing of civil proceedings.[65] However, it noted that Article 13(1) of the Data Protection Directive, referred to in Article 15(1), allows Member States to restrict the confidentiality obligation when necessary to "protect the rights and freedoms of others". The Court consequently held that Article 15(1) "must be interpreted as expressing the Community legislature's intention not to exclude from [its] scope the protection of the right to property, or situations in which authors seek to obtain that protection in civil proceedings". The conclusion was therefore reached that the E-Privacy Directive neither precludes Member States from laying down an obligation to disclose personal data in the context of civil proceedings, nor does it compel Member States to impose such an obligation. It is therefore a necessary consequence of the judgment that the levels of protection of intellectual property rights and data protection will vary amongst Member States depending on how the balance referred to by the Court is struck at national level.[66] These disparities will, as Groussot highlights, "endanger the coherence of the internal market".[67]

One recent case seems, at first glance, to buck this trend by emphasising the Data Protection Directive's harmonisation role. Article 7 of the Directive sets out six principles, one of which must be fulfilled in order to legitimise data processing. The first of these principles is that the data subject's consent is acquired prior to processing; the other legitimising principles do not require consent. In the *ASNEF*[68] case the Spanish referring court queried whether Member States are entitled to add extra conditions to those required by Article 7 of the Directive. The Spanish legislation at stake provided that the principles which legitimise data processing in the absence of consent could apply only if the relevant data appeared in public sources; a condition not required by the Directive.[69] In providing a response to the national court, the Court of Justice highlighted that the Directive aimed to achieve complete harmonisation, rather than a minimum level of harmonisation.[70] It followed from this objective that Article 7 "sets out an exhaustive and restrictive list of cases in which the

[65] Ibid, §52.

[66] See, for instance, Kuner who states that "the ECJ's judgment may lead to a further fragmentation of the law, in which some Member States allow such use of personal data (i.e. Its disclosure for the purposes of pursuing civil infringements) but others do not". Kuner, "Data protection and rights protection on the Internet: the *Promusicae* judgment of the European Court of Justice" (2008) 30(5) *European Intellectual Property Review* 199.

[67] Groussot, "Music Production in Spain *(Promusicae) v. Telefónica de España SAU*, – *Rock the KaZaA: Another Clash of Fundamental Rights*", (2008) 45(6) *Common Market Law Review* 1745, 1765.

[68] C-468/10 *Asociación Nacional de Establecimientos Financieros de. Crédito (ASNEF) v Administración del Estado* [2011] ECR I-0000.

[69] Ibid, §17.

[70] Ibid, §29.

processing of personal data can be regarded as being lawful".[71] The margin of discretion granted to Member States by the Directive could be exercised only in accordance with "the objective pursued by Directive 95/46 of maintaining a balance between the free movement of personal data and the protection of private life".[72] The Court considered that a distinction must be made between "national measures that provide for additional requirements amending the scope of a principle referred to in Article 7 of Directive 95/46, on the one hand, and national measures which provide for a mere clarification of one those principles, on the other hand".[73]

The significance of this case is not such as to detract from the previous assertion that the Court has loosened the links between the Directive and its market harmonisation objectives. By adding restrictive conditions to a Directive that was designed to ensure maximum harmonisation, the Spanish authorities impeded the Directive's harmonising objectives in an obvious manner which was bound to be sanctioned by the Court. This textbook example of a hindrance to inter-State movement cannot be compared to the factual scenarios in *Satamedia* and *Promusicae* where the Court could have been expected to defend the Directive's market harmonisation aims rather than granting the national authorities unlimited discretion when it came to the interpretation of key exceptions to the Directive.

Before moving on, one final point should be made about *Satamedia* and *ASNEF*. In both, the Court of Justice referred to the objective of the Directive in the singular, rather than in the plural, by amalgamating its free movement and fundamental rights aims. In *Satamedia* the Court emphasised the free movement aspect saying that the objective of the Directive was "to provide for the free flow of personal data whilst protecting the fundamental rights of persons". In *ASNEF* the Court said that Directive's objective was "maintaining a balance between the free movement of personal data and the protection of private life".[74] The entry into force of the Lisbon Treaty has separated these two aims, with the protection of the right to data protection viewed as an end of itself. This development will be discussed in the following section.

3.4 The Rights-Based Approach to Data Protection in the EU and the Residual Impact of Market Integration Restraints

3.4.1 Data Protection as a Fundamental Right Pre-Lisbon

The abovementioned judgments had the effect of distancing European data protection legislation from its internal market objective. However, this did not lead to the bolstering by the Court of the fundamental rights objective of data protection legislation, at least not immediately. It is argued here that prior to the entry into force of the

[71] Ibid, §30.

[72] Ibid, §34.

[73] Ibid, §35.

[74] Ibid, §34.

Lisbon Treaty the Court of Justice detracted from data protection's fundamental rights dimension by (i) weakening the right to data protection when it conflicted with other rights of constitutional significance. Moreover, it limited data protection's potential as an independent right by equating it to the right to privacy (ii).

(i.) Weakened Data Protection in Light of Conflicting Objectives
One trend that is arguably evident in the Court's pre-2009 case law on data protection is that the protection offered to individuals by data protection legislation is watered down when data protection enters into conflict with other rights and values. In *Satamedia*, as mentioned above, the Court did not grant sufficient weight to the right to data protection vis-à-vis freedom of expression. The Court's interpretation of the exception for journalistic purposes, in particular its failure to specify that the matters reported must be of public concern, is at odds with the ECtHR's interpretation of the concept of freedom of expression.[75] Similarly in *Promusicae* the Court attempted to strike a balance between the right to property of intellectual property rights holders and the right to data protection of internet users. Striking the correct balance between these rights is a daunting task. On the one hand, "consumers will only readily take up new digital services if they are reassured that their personal data is sufficiently protected and not abused for marketing purposes or worse".[76] On the other hand, the protection of intellectual property rights arguably benefits society as a whole as without adequate protection, copyright owners would lack the incentive to innovate or the ability to earn a living.[77] The Court, however, did not decide how to strike a balance between the two instead preferring to delegate this tricky task to national authorities. It is therefore entirely possible that national regimes could promote the effective enforcement of intellectual property rights to the detriment of the individual's right to data protection. Finally, in *Bavarian Lager* (which will be discussed presently) the General Court ensured that an individual's right of access to documents trumped the right to data protection as long as the data subject's right to privacy was not violated.

(ii) The conflation of the rights to data protection and privacy
It is arguable that a second trend also emerges in the Court's pre-Lisbon Treaty data protection case law; the Court consistently conflated the right to data protection and the right to privacy.[78] In *Promusicae*[79] the national referring court

[75] Oliver, *o.c.*, 1462.

[76] Koempel, "Data Protection and Intellectual Property" (2005) 11(6) *Computer and Telecommunications Law Review* 185, 185.

[77] Wei, "ISP indirect copyright liability: conflicts of rights on the internet", (2009) 15(8) *Computer and Telecommunications Law Review* 181, 181/

[78] This author advocates that while in many instances data protection ensures privacy objectives, data protection also ensures independent objectives which privacy does not, for instance, counterbalancing information asymmetries between data processors and data subjects. For a thorough discussion of the distinction between the two rights see Nadezhda Purtova, *Property Rights in Personal Data: a European Perspective,* Kluwer Law International, 2011, 217–220.

[79] *Promusicae o.c.*

made no allusion to data protection in its preliminary reference however the Court raised data protection issues of its own motion. It stated that "the situation in respect of which the national court puts that question involves (…) a further *fundamental right*, namely the right that guarantees protection of personal data and hence of private life".[80] Although this *ex officio* reference to data protection as a fundamental right was seemingly promising, the Court's statement is also an example of the Court's tendency to conflate the rights to privacy and the data protection.

In *Österreichischer Rundfunk*, for instance, when examining the compatibility of the national auditing activity with the Directive, the Court emphasised that the provisions of the Directive must be interpreted in light of fundamental rights, in particular privacy. Therefore "for the purposes of applying the Directive", the Court systematically examined whether there had been an interference with private life contrary to Article 8 ECHR and, if so, whether it was justified. In so doing, the Court of Justice completely overlooked the specific guidelines set out in the Directive leading one author to question the relevance of the Directive if the interpretation of Article 8 ECHR alone is decisive in the event of a dispute.[81] While on the facts of *Rundfunk* such heavy reliance on the right to privacy led to the same outcome that would have been achieved by relying on the Directive, this may not always be so and the Court should have exercised more caution in substituting the application of secondary legislation with the application of a general principle of EU law. Indeed, the Court in *Rundfunk* inadvertently highlights a situation when the application of the two rights could differ. It notes that "the mere recording by an employer of data by name relating to the remuneration paid to his employees cannot as such constitute an interference with private life" under Article 8 ECHR; such recording would however constitute data processing for the sake of the Directive and would need to comply with its principles.

In *Bavarian Lager*[82] the General Court's consideration of how to reconcile the rights of data protection and access to documents (a right which is not enshrined in the ECHR but is set out in the Charter[83]) also centred on the right to privacy. In that case, the General Court was asked to consider whether the European Commission's decision to provide Bavarian Lager with the minutes of a meeting it requested via European Access to Documents legislation (Regulation 1049/2001[84]) in an anonymised form struck the right balance between freedom of information and data protection in the EU legal order. Article 4(1)(b) of Regulation 1049/2001 is the only provision that regulates the relationship between the two. According to this article, a request for access to a document shall be refused where the document's disclosure

[80] Ibid, §63.

[81] Classen, *o.c.*, 1383.

[82] T-194/04 *Bavarian Lager v Commission* [2007] ECR II-3201.

[83] European Union, *Charter of Fundamental Rights of the European Union*, [2000] OJ C 364/01.

[84] Regulation (EC) No 1049/2001 of the European Parliament and of the Council of 30 May 2001 regarding public access to European Parliament, Council and Commission documents [OJ] L 145/43.

would undermine the protection of "privacy and the integrity of the individual, in particular in accordance with Community legislation regarding the protection of personal data". The General Court therefore analysed whether the disclosure of names of those attending a European Commission meeting would breach Article 8 ECHR. It concluded that it would not and therefore that the Article 4(1)(b) exception was not applicable.[85] Consequently, the General Court held that the application to the request of the "additional conditions" set out in the European data protection legislation concerned,[86] such as the need for consent of the data subject, would be contrary to the objective of Regulation 1049/2001.[87] The General Court therefore annulled the Commission decision.

The reasoning of the General Court in this case is very clear-cut; there was no violation of the right to privacy, therefore the data protection rules do not apply. While at first glance this could be confused for another example of the conflation of the rights to data protection and privacy, it is in fact the opposite. The Court examined whether or not the data subjects' Article 8 ECHR right to privacy had been violated. The wording of Article 4(1)(b) of Regulation 1049/2001 provides that in cases of conflict between data protection and freedom of information, the data protection rules prevail when privacy is undermined. The Court's judgment therefore implicitly acknowledges that not all data processing adversely affects the right to privacy and, consequently, that data protection applies to a wider variety of personal data than privacy law. While De Hert and Gutwirth conclude that the ease with which the General Court distinguished between two types of personal data (those that are protected by the right to privacy and those that are not) "does not sit comfortably with the formal constitutional codification of data protection within EU law",[88] it is arguable that such a distinction in fact reinforces data protection's status as a constitutional right. It liberates it from the right to privacy, paving the way for the emergence of an independent right (the objectives of which remain to be elaborated upon, as will be seen below).

3.4.2 The Right to Data Protection in the Post-Lisbon Era

In this section, it will be demonstrated that the Court is (i) keen to endorse the right to data protection in the EU legal order (ii) however the Court's insistence on

[85] *Bavarian Lager,* §132–133.

[86] Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data [OJ] L8/1.

[87] *Bavarian Lager,* §137.

[88] De Hert and Gutwirth, "Data Protection in the in the case law of Strasbourg and Luxemburg: Constitutionalisation in Action" in Gutwirth, Poullet, De Hert, Nouwt & De Terwangne (eds), *Reinventing Data Protection*? Dordrecht, Springer, 2009, 41.

conflating the rights to data protection and privacy has the potential to limit the development of an independent right to data protection and to therefore preclude the need for consideration of its (distinct, but sometimes overlapping) objectives.

(i) Endorsing the Right to Data Protection in the EU Legal Order
The Lisbon Treaty, which entered into force on 1 December 2009, revolutionised the role of data protection in EU law in a number of ways. For instance Article 16 TFEU provides for a directly effective[89] right to data protection by stating that "[e]veryone has the right to the protection of personal data concerning them". This provision can also act as a legal basis for data protection legislation in the future, freeing such legislation from internal market constraints. Moreover, the human rights credentials of the EU have been significantly reinforced. Not only can the Union become a signatory of the ECHR[90] but its Charter of Fundamental Rights[91] is now legally binding primary law.[92] The Charter sets out a right to privacy in its Article 7[93] but also includes a separate right to data protection in its Article 8.[94] The inclusion of a right to data protection in the Charter differentiates it from other key human rights documents[95] which consider data protection as a subset of the right to privacy.[96] Therefore, it is unsurprising that the Court has shown considerable enthusiasm for the right to data protection following the entry into force of the Lisbon Treaty.

[89] Article 16 TFEU is clear, precise and unconditional and therefore fulfils the conditions for direct effect. The European Data Protection Supervisor (EDPS) has indicated that this provision is directly effective in his speech entitled "Data Protection in the Light of the Lisbon Treaty and the Consequences for Present Regulations" delivered at the 11th Conference on Data Protection and Data Security in Berlin on 8 June 2009. (Accessed via http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Speeches/2009/09-06-08_Berlin_DP_Lisbon_Treaty_EN.pdf)

[90] Official negotiations for ratification of the ECHR began on 7 July 2010. However this process has stalled since the October 2011 submission of a draft Treaty to the Committee of Ministers of the Council of Europe by the Steering Committee for Human Rights. See, European Court of Human Rights, Solemn hearing of the European Court of Human Rights on the occasion of the opening of the judicial year, Friday 27 January 2012, address by Sir Nicolas Bratza, President of the European Court of Human Rights. (Accessed on 15 April 2012, http://www.echr.coe.int/ECHR/EN/Header/The+Court/Events+at+the+Court/Opening+of+the+judicial+year/).

[91] European Union, *Charter of Fundamental Rights of the European Union, o.c.*

[92] The Charter was previously only binding on the EU Institutions and Member States.

[93] Article 7 provides that "Everyone has the right to respect for his or her private and family life, home and communications".

[94] Article 8(1) stipulates that "Everyone has the right to the protection of personal data concerning him or her". This right is elaborated upon in Article 8(2) which provides that the data "must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law" and that "everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified".

[95] Such an independent right exists at national level in some Member States. For instance, Article 35 of the Portuguese Constitution was amended in 1997 to include a right to data protection.

[96] EU Agency for Fundamental Rights, 'Data Protection in the European Union: the role of National Data Protection Authorities – Strengthening the fundamental rights architecture in the EU II', 6, (Accessed via www.fra.europa.eu/fraWebsite/attachments/Data-protection_en.pdf).

A clear signal that data protection was being considered in new light came with the Court's judgment in *Volker und Markus Schecke*[97] when the Court held, for the first time, that provisions of European secondary legislation were invalid as they interfered with rights guaranteed by the Charter. The rights at stake in this case were the rights to data protection and privacy. A German court referred a number of questions concerning the validity of an EU requirement that information concerning the beneficiaries of funding derived from certain Common Agricultural Policy funds be made publicly available by each Member State via a searchable website. In particular, it sought to know whether such a requirement was compatible with European data protection law. The Court held that the publication of this data constituted an interference with the data subjects' rights under Articles 7 and 8 of the Charter. It then considered whether this interference could be justified. Unlike the Advocate General who was highly critical of the inability of the European institutions to accurately define the objectives of the transparency legislation, the Court accepted the objectives advanced by the institutions without question. It then considered whether the interference with the rights to data protection and privacy were proportionate to the numerous objectives pursued by the transparency initiatives.

The Court engaged in a meticulous proportionality analysis and found that the transparency initiatives were suitable but not necessary to achieve their objectives. It recalled that "derogations and limitations in relation to the protection of personal data must apply only in so far as is strictly necessary" and that "it is possible to envisage measures which affect less adversely that fundamental right of natural persons and which still contribute effectively to the objectives of the EU rules in question".[98] Indeed, the Court itself suggested alternative more 'data protection-friendly' methods that could have been used by the Council and the Commission.[99] Therefore, the manner in which the Court resolves this "constitutional issue"[100] (namely whether the objective of achieving transparency in the management of CAP finance may override the individual's rights to data protection and privacy) illustrates that the Court is no longer reluctant to take a stand on conflicts between the right to data protection and other important interests. Indeed, the hardcore proportionality analysis engaged in by the Court in *Volker* stands in marked contrast with the Court's failure, outlined above, to provide adequate guidance to the national court in *Promusicae*. Furthermore, the Court's willingness to apply the provisions of the Charter, rather than the ECHR, to the case before it is to be welcomed. Indeed, this was so even though the Charter was not in force at the time of the contested data processing.

---

[97] C-92/09 and C-93/09 *Volker und Markus Schecke* [2010] ECR I-000. See Eva Nanopoulos, "It is Time, Charter, Rise and Shine" (2011) 70 *Cambridge Law Journal* 306.

[98] *Volker, o.c.,* §87.

[99] Ibid, §81.

[100] Opinion of Advocate General Sharpston delivered on 17 June 2010 in C-92/09 and C-93/09 *Volker und Markus Schecke*, §2.

(ii) Stunting the Development of this Newborn Right
Despite the promising changes that the Lisbon Treaty brought into force, and the Court's subsequent endorsement of the right to data protection, there is still room for improvement in the Court's jurisprudence.

In the Court of Justice's *Bavarian Lager*[101] judgment on appeal, the Court held that the General Court had erred in law by limiting the application of Article 4(1)(b) to situations in which Article 8 ECHR is breached. It found that data processing activities cannot be separated into two categories; those examined in light of the ECHR right to privacy and those examined for compliance with European data protection legislation.[102] Therefore, it concluded that in all situations where access is sought to a document containing personal data the Data Protection Directive becomes applicable in this entirety.[103] It follows from this that even when the right to privacy of the individual data subjects is not infringed (as was arguably the situation in *Bavarian Lager*), the data protection rules must be complied with before access is granted to the requested document(s). Data protection rules therefore trump access to document rules even when there is no privacy interest at stake. What then are the other objectives of data protection (in addition to privacy) that allow the Court to override the right to access to documents (also enshrined in the Charter) so easily? The Court overlooked this golden opportunity to actually explain the differences between the two rights; data protection and privacy.

It would seem from the Court's judgment in *Volker* that this is because the Court is, at best, unclear about the relationship between the two rights. It firstly states that they are "closely connected"[104] but then soon thereafter considers them to be a hybrid species when it refers to "the right to respect for private life with regard to the processing of personal data, recognised by Articles 7 and 8 of the Charter".[105] Equally problematic is that it erroneously borrows from the European Court of Human Rights' (ECtHR) Article 8 ECHR case law and applies this to both of the Charter Articles. It states that Article 7 and 8 rights concern "any information relating to an identified or identifiable individual" and cites *Amann v. Switzerland* and *Rotaru v. Romania* as authority.[106] However, this case law does not support the proposition that Article 8 ECHR applies to "any information relating to an identified or identifiable person". Rather, this is how the Data Protection Directive defines "personal data". Indeed, despite the ECtHR's expansive interpretation of the right to privacy, it is frequently advocated that the right to privacy does not apply to the same wide range of data that the data protection rules apply to.[107]

---

[101] C-28/08 *European Commission v. Bavarian Lager* [2010] ECR I-6055.

[102] *Bavarian Lager*, §58–61.

[103] Ibid, §63.

[104] *Volker, l.c.,* §47.

[105] Ibid, §52.

[106] Ibid.

[107] See, for instance, Opinion of the Article 29 Working Party, "Opinion 4/2007 on the concept of personal data", 20 June 2007, 01248/07/EN WP 136, or Kranenborg, "Access to documents and data protection in the European Union: on the public nature of personal data" (2008) 45(4) *Common Market Law Review* 1079, 1091.

In contrast, in her Opinion in *Volker* Advocate General Sharpston clearly distinguishes between data protection and privacy when she states that "[t]wo separate rights are here invoked: a classic right (the protection of privacy under Article 8 ECHR) and a more modern right (the data protection provisions of Convention No 108)".[108] Similarly, Schwartz and Reidenberg have noted that calling data protection "information privacy" is an attempt to "put new wine in old bottles"[109] Indeed, by conflating these rights the Court risks subjecting the modern right of data protection to the limitations that have been imposed on the 'classic' right to privacy thereby stunting its development. It also precludes debate, both inside and outside the Court, of what independent objectives data protection pursues and how best to reconcile these objectives with competing rights and interests. Surely this was a danger that the drafters of the European Charter sought to avoid when they enumerated the rights separately in the first instance.

3.5 Conclusion: Casting Our Eyes on the Future

This paper set out to demonstrate two points. Firstly, that the ambiguous relationship between the Directive's dual objectives could lead to doubts concerning its validity. It is difficult to conclude, particularly with the benefit of hindsight, that the Directive's fundamental rights objective was ever secondary or merely ancillary to its free movement objective. If this is indeed the case then the elevation of data protection to the status of fundamental rights by the Charter, which was drafted only 5 years after the Directive entered into force, is all the more remarkable. The Court of Justice has never been asked explicitly to consider whether the EU exceeded its competence by relying on a single legal basis for the legislation; the Court would have been compelled to consider the relationship between the two objectives if this were the case. However, from a practical perspective this question is now moot as Article 16 TFEU provides a legal basis for data protection measures therefore resort will no longer be had to Article 114 TFEU.

Secondly, this paper sought to demonstrate that while the Directive's market-making characteristics have been interpreted loosely by the Court, its fundamental rights characteristics have become increasingly prominent in the post-Lisbon era. A note of caution was, however, sounded on this point. Although the Court has shown a willingness to emphasise data protection's fundamental rights aspects, it is seemingly uncertain as to whether there is more to the right to data protection than privacy protection.

One common theme therefore emerges from this paper; data protection has suffered an identity crisis before the Court of Justice. The objectives of EU data protection

[108] Opinion of Advocate General Sharpston in *Bavarian Lager, o.c.*, §71.

[109] Quoted by Purtova, *o.c.*, 90.

law have been unclear from the outset. This uncertainty is evident in the earlier cases where the link between fundamental rights and the directive's market harmonisation objectives was in question. However, it is also visible in later cases where the Court attempts to balance data protection with other rights. In *Bavarian Lager* the Court was critical of the General Court's attempt to balance freedom of information and data protection concerns by allowing the former to prevail when individual privacy is not undermined. It preferred to let data protection prevail in all circumstances. However, why should data protection trump access to documents in all instances, even when privacy is not undermined? Privacy aside, what other objectives does data protection serve? The Court provides no answers to these questions.

The introduction of an explicit legal basis for data protection legislation has paved the way for the Court to consider the objectives of data protection more explicitly. Equally, the Charter – with its separate rights to data protection and privacy – could provide the Court with the chance to shed some much needed light on the concrete objectives of European data protection. This opportunity has been overlooked to date with the Court treating the rights to data protection and privacy as some form of hybrid. The impetus to define the objectives of data protection law is however more present now than ever before. The European Commission's Proposed Regulation[110] seeks to bolster both the market harmonisation and fundamental rights objectives of data protection. Its rights protection objectives are promoted as new rights are introduced,[111] old rights are reinforced[112] and more effective enforcement mechanisms[113] are set out. Harmonisation objectives are facilitated by new institutional mechanisms put in place to ensure the harmonious application of the law; the concept of "lead authority",[114] the consistency mechanism,[115] the role of the European Data Protection Board in ensuring consistency[116] to name but a few. Most importantly however is the choice of legislative instrument: a regulation rather than a directive. A regulation will play a crucial role in achieving the uniform application of data protection rules across the EU. Nevertheless, it is advocated that this uniformity will increasingly lead to tensions between the Member States as to how to correctly strike the balance between data protection and competing rights and interests. Therefore, without a clear vision of the objectives of EU data protection law, the Court of Justice will be unable to coherently guide the development of EU data protection law in the future.

---

[110] Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data COM (2012) 11 final ("Proposed Regulation").

[111] For instance, the Article 18 "right to data portability".

[112] For example, the fortification of the right to erasure in Article 12(b) of the Data Protection Directive by the introduction of a "right to be forgotten" in Article 17.

[113] For example, Article 79 sets dissuasive administrative sanctions (which could be as much as 2% of a companies annual global turnover). Under Directive 95/46 EC such sanctions were implemented by Member States and therefore they varied widely.

[114] Proposed Regulation, *o.c*, Article 51.

[115] Ibid, Article 57.

[116] Ibid, Article 58.

References

Amended proposal for a Council Directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data. *COM* (92) 422 final.

Bainbridge, David. 2005. *Data protection*, 2nd ed. Welwyn: xpl publishing.

Barnard, C. 2010. *The substantive law of the European Union*, 2nd ed. Oxford: Oxford University Press.

Broberg, Morten P., and Niels Fenger. 2010. *Preliminary references to the European court of justice*. Oxford: Oxford University Press.

Classen, C.D. 2004. C-139/01 Österreichischer Rundfunk and others: Case-note. *Common Market Law Review* 41(5): 1377.

Council of Europe. Convention for the protection of individuals with regard to automatic processing of personal data, ETS No.108, 28.I.1981.

De Hert, Paul, and Serge Gutwirth. 2009. Data protection in the in the case law of Strasbourg and Luxemburg: Constitutionalisation in action. In *Reinventing data protection?* ed. Serge Gutwirth, Yves Poullet, Paul De Hert, Sjaak Nouwt, and Cecile De Terwangne, 41. Dordrecht: Springer.

EDPS. 2009. "Data protection in the light of the Lisbon treaty and the consequences for present regulations" delivered at the *11th conference on data protection and data security* in Berlin on 8 June 2009.

EU Agency for Fundamental Rights. 'Data Protection in the European Union: the role of National Data Protection Authorities – Strengthening the fundamental rights architecture in the EU II', 6, www.fra.europa.eu/fraWebsite/attachments/Data-protection_en.pdf.

European Commission. Communication on the protection of individuals in relation to the processing of personal data in the Community and Information Security. *COM* (90) 314 final.

European Commission. Community policy for data processing. *COM* 75 (467) final.

European Commission. Communication to the Council on a Community Data-Processing Policy SEC (73) 4300 final

European Commission. Recommendation of 29 July 1981 relating to the Council of Europe Convention for the protection of individuals with regard to automatic processing of personal data [1981] OJ L246/31.

European Court of Human Rights. Solemn hearing of the European Court of Human Rights on the occasion of the opening of the judicial year, Friday 27 January 2012, address by Sir Nicolas Bratza, President of the European Court of Human Rights.

European Parliament. Resolution on the Protection of the Rights of the Individual in the Face of Developing Technical Progress in the Field of Automatic Data Processing [1975] OJ C60/48.

European Parliament and Council Directive 95/46/EC of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L281/23.

European Union. Charter of Fundamental Rights of the European Union, [2000] OJ C 364/01.

Groussot, X. 2008. Music production in Spain *(Promusicae) v. Telefónica de España SAU*, *– Rock the KaZaA: Another clash of fundamental rights*. *Common Market Law Review* 45(6): 1745.

Hijmans, Hielke, and Alfonso Scirocco. 2009. Shortcomings in EU data protection in the third and second pillars. Can the Lisbon treaty be expected to help? *Common Market Law Review* 46(5): 1485.

Koempel, Florian. 2005. Data protection and intellectual property. *Computer and Telecommunications Law Review* 11(6): 185.

Kranenborg, Herke. 2008. Access to documents and data protection in the European Union: On the public nature of personal data. *Common Market Law Review* 45(4): 1079.

Kuner, Christopher. 2008. Data protection and rights protection on the internet: The *Promusicae* judgment of the European court of justice. *European Intellectual Property Review* 30(5): 199.

Nanopoulos, Eva. 2011. It is time, charter, rise and shine. *Cambridge Law Journal* 70: 306.

OECD. Guidelines Governing the Protection of Privacy and the Transborder Flows of Personal Data, 23 Sept 1980.

Oliver, Peter. 2009. The protection of privacy in the economic sphere before the European court of justice. *Common Market Law Review* 46(5): 1443.

Opinion of the Article 29 Working Party. Opinion 4/2007 on the concept of personal data, 20 June 2007, 01248/07/EN WP 136.
Proposal for a Council Directive concerning the protection of individuals in relation to the processing of personal data OJ C 277/3.
Proposal for a Council Directive concerning the protection of personal data and privacy in the context of public digital telecommunications networks, in particular the integrated services digital network (ISDN) and public digital mobile networks OJ C 277/12.
Proposal for a Council Decision in the field of Information Security OJ C 277/18.
Purtova, Nadezhda. 2011. *Property rights in personal data: A European perspective*. Alphen aan den Rijn: Kluwer Law International.
Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data [OJ] L8/1.
Regulation (EC) No 1049/2001 of the European Parliament and of the Council of 30 May 2001 regarding public access to European Parliament, Council and Commission documents [OJ] L 145/43.
Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data COM (2012) 11 final.
Rule, James B., and Graham Greenleaf. 2008. *Global privacy protection: The first generation*. Cheltenham: Edward Elgar Publishing.
Wei, Weixiao. 2009. ISP indirect copyright liability: Conflicts of rights on the internet. *Computer and Telecommunications Law Review* 15(8): 181.

Case Law of the Court of Justice

C-468/10 *Asociación Nacional de Establecimientos Financieros de. Crédito (ASNEF) v Administración del Estado* [2011] ECR I-0000.
C-92/09 and C-93/09 *Volker und Markus Schecke* [2010] ECR I-0000.
Opinion of Advocate General Sharpston delivered on 17 June 2010 in C-92/09 and C-93/09 *Volker und Markus Schecke*.
C-28/08 *European Commission v. Bavarian Lager* [2010] ECR I-6055.
C-73/07 *Tietosuojavaltuutettu* v. *Satakunnan Markkinapörssi OY*, *Satamedia* [2008] ECR I-09831.
Opinion of Advocate General Kokott delivered on 8 May 2008 in C-73/07 *Tietosuojavaltuutettu* v. *Satakunnan Markkinapörssi OY*, *Satamedia*.
C-275/06 *Productores de Música de España (Promusicae) v. Telefónica de España* [2008] ECR I-271.
C-438/05 *International Transport Workers' Union v Viking Line* [2007] ECR I-10779.
C-431/05 *Laval un Partneri Ltd v Svenska Byggnadsarbetareförbundet* [2007] ECR I-11767.
T-194/04 *Bavarian Lager v Commission* [2007] ECR II-3201.
C-36/02 *Omega Spielhallen- und Automatenaufstellungs-GmbH v Oberbürgermeisterin der Bundesstadt Bonn* [2004] ECR I-9609.
C-491/01 *Queen v. Secretary of State for Health, ex parte British American Tobaco (Inv) Ltd & Imperial Tobacco Ltd.* 2002 ECR I-11453.
C-139/01 *Österreichischer Rundfunk and Others* [2003] ECR I-4989.
Opinion of Advocate Generak Tizzano delivered on 14 November 2002 in C-139/01 *Österreichischer Rundfunk and Others*.
C-101/01 *Bodil Lindqvist* [2003] ECR I- 12971.
Opinion of Advocate General Tizzano delivered on 19 September 2002 in C-101/01 *Bodil Lindqvist*.
C-60/00 *Carpenter* [2002] ECR I-6279.

C-112/00 *Eugen Schmidberger Internationale Transporte und Planzüge v Republic of Austria* [2003] ECR I-5659.
Opinion 2/00 [2001] ECR I-9713.
Opinion 2/94 [1996] ECR I-1759.
C-300/89 *Commission v Council (Titanium Dioxide)* [1991] ECR I-2867.
C-66/85 *Lawrie- Blum v. Land Baden-Württemberg* [1986] ECR 2121.
C-5/88 *Wachauf* [1989] ECR I-2609.
C-4/73 *Nold* [1974] ECR 491.
C-11/70 *Internationale Handelsgessellshaft* [1970] ECR 1125.
C-7/68 *Commission v. Italy (the art treasures case)* [1968] ECR 423.

Chapter 4
Anonymity: A Comparison Between the Legal and Computer Science Perspectives

Sergio Mascetti, Anna Monreale, Annarita Ricci, and Andrea Gerino

4.1 Introduction

There are two opposing interests in our society: on one side, there is the need to collect and share information, which are activities that enable a number of services aimed at economic profit, scientific research, etc. On the other side, the right to personal data protection, intended as the right of disposal over all data in connection with our personality, requires to safeguard the subjects whose information is collected and shared. This contrast is one fragment of a broader problem concerning the relationship between law and technology. The overall question is whether legal definitions should adapt to technical solutions or if, vice versa, technology should implement the regulations in force. Certainly, the technological developments in the Internet era pose new questions to researchers in the two communities involved: Law and Computer Science. In this view, the topic of this paper, i.e., anonymity as a tool to guarantee personal data protection, is emblematic of the need for constant exchange of ideas and collaboration between these two communities.

The problem is that, despite the great research effort of both communities in the privacy protection field, most of the contributions address the problem either from the legal or the technical point of view only. This attitude has led to the

S. Mascetti (✉) • A. Gerino
Dipartimento di Informatica, University of Milan, Milan, Italy
e-mail: sergio.mascetti@di.unimi.it; andrea.gerino@di.unimi.it

A. Monreale
Department of Computer Science, University of Pisa, Pisa, Italy

Dipartimento di Informatica, University of Pisa, 3, Largo Pontecorvo, 56127 Pisa, Italy
e-mail: amonreale@di.unipi.it

A. Ricci
Department of Juridical Sciences "A. Cicu", University of Bologna, Bologna, Italy
e-mail: annarita.ricci@unibo.it

S. Gutwirth et al. (eds.), *European Data Protection: Coming of Age*,
DOI 10.1007/978-94-007-5170-5_4,

specification of basic definitions and objectives that only partially overlap, hence raising difficulties in communication and in the reciprocal applicability of the research results.

In contrast with this tendency, Ohm discusses the legal definitions of privacy, starting from the analysis of the contributions in the Computer Science community.[1] The conclusion presented in this paper is surprising: privacy law should not rely on the concept of anonymity. Jane Yakowitz's study[2] also leads to surprising conclusions. This paper addresses the problem of data anonymization for research purposes and it concludes that, since current privacy policies overtax valuable research without reducing any realistic risks, law should provide a safe harbour for the dissemination of research data and technical solutions are not necessary. In a recent paper, Schwartz et al.[3] support the idea that the concept of anonymity should be part of privacy laws, but its definition should be "reconceptualized". In these three papers, the interest resides, from our point of view, in their interdisciplinary approach.

With the aim to continue in the same direction, in this paper we attempt to integrate research on personal data protection in the two areas of Computer Science and Law. The approach is to address the central concept of anonymity from both perspectives, by reciprocally explaining the most important concepts, finding correspondences in the terminology and highlighting points in common and differences in the two areas. To achieve this, we first analyze the legal definitions of anonymous datum, as specified in the European Directive (Sect. 4.2). Then, we describe the main models and techniques proposed in the Computer Science literature to target the problem of anonymity (Sect. 4.3). Since this description of the state of the art in the two areas is targeted to readers in both communities, it focuses more on the main concepts and results, rather than on the technical details. We then discuss one similarity and some differences between the assumptions and definitions adopted by the two communities and the consequential results (Sect. 4.4). In particular, we focus on four main topics:

1. the role of anonymity in privacy preservation,
2. the relationship between identifying information and personal data,
3. the measurement of anonymity,
4. the relationship between anonymity and the principle of minimization.

We conclude that, despite there being some analogies, there are also a number of gaps, that on one side render some of the technical solutions not directly applicable to the regulations in force and, on the other side, suggest some specific interpretations

[1] Paul Ohm, "Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization," *UCLA Law Review, Vol. 57, p. 1701, 2010* (2009).

[2] Jane Yakowitz, "Tragedy of the Data Commons," *Harvard Journal of Law and Technology, Vol. 25, 1, 2011*.

[3] Paul M. Schwartz and Daniel J. Solove, "The PII Problem: Privacy and a New Concept of Personally Identifiable Information," *New York University Law Review, Vol. 86, 2011* (2011).

of the current regulations in order to make them adequate to the existing technical solutions. Rather than a point of arrival, these conclusions are meant to be a starting point for discussion and integration between the two communities. In fact, thanks to its interdisciplinary character, this work tries to break down the communication barrier or at least the difficulties in dialogue between the two communities. The growing need of both communities for a systematic and interdisciplinary analysis of the anonymity notion and its use in protecting personal data can be adequately satisfied only through the development of a common language or at least a thorough understanding of the different approaches.

4.2 The Notion of Anonymity in European Legislation on Personal Data

The concept of anonymity has gained particular importance in relation to the application of European legislation on personal data. Indeed, while regulations apply to personal data, anonymous data are excluded from their field of application. This section analyses the legal understanding of anonymity, in particular with respect to the European Directive on personal data protection, and it tries to answer the following main questions:

- What is the interpretation of anonymity in common language?
- Should anonymity be considered a relative or absolute concept?
- What does anonymous data mean in legal terms?

To achieve this, we start with the notion of anonymity in common language (Sect. 4.2.1). Then we describe how the European legislation on personal data captures this concept.[4,5] Following the same approach of European legislation, we first introduce the concept of personal data (Sect. 4.2.2) and then proceed to defining anonymous data (Sect. 4.2.3). In order to show how European legislation has been implemented into national laws, we report the example of the anonymous data definition in the Italian Personal Protection Code (Sect. 4.2.4). The reason for choosing the Italian Personal Code is that it can be considered a "rigorous" implementation of the European Directive.

Before we proceed with the analysis, it is necessary to point out that, when we refer to the subjects of data processing, we use the definitions stated in Directive

[4] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281, 23.11.1995, 31–50.

[5] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), OJ L 201, 31.7.2002, 37–47.

95/46/EC: the *controller* is an entity (i.e., a natural or legal person, public authority, agency or any other body) that, alone or jointly with others, determines the purposes and means of personal data processing; the *processor* is an entity that processes personal data on behalf of the controller; the *recipient* is an entity to whom data are disclosed, whether a third party or not, and, finally, the *data subject* is the person to whom the personal data refer to.

4.2.1 The Notion of Anonymity in Common Language

In common language, the meaning of anonymity comes from the etymology of the term, that is, literally, "without name". "The word denotes an absolute concept: an anonymous person is one, of whom you do not know anything, somebody you cannot recognize or identify".[6] The definition of anonymity as an absolute concept is often taken for granted in the common understanding. However, as we will subsequently explain, anonymity in the legal context is actually a relative concept. Indeed, anonymity is often relative to specific facts, subjects and purposes. A musical arrangement, for instance, may be anonymous for a person but not for another, depending on whether this person knows the author. So the right to be anonymous, when recognized, refers to certain subjects, in predefined circumstances and for specific occasions, which can be specified by the law.[7] For example, the Italian legal system recognizes the biological mother's right not to be named in her son's birth certificate.

The transferral of the anonymity notion from common language to the legal context is not immediate. This is due to two main reasons. First, legal reasoning needs a degree of precision that is not generally required in common language. For instance, in legal terms it is necessary to specify the conditions that make a datum anonymous. Second, while the terms "anonymous" and "anonymity" are used in legal texts, they seem to have non-homogeneous values in the different legal sectors. In particular, we find references to the term "anonymous" in private law (copyright), criminal law (as an aggravating circumstance in some threat crimes), administrative law (open competitions for public recruitment) and constitutional law (freedom of expression). Consequently, we can conclude that the term "anonymity" is used in various areas but with a different slant, which makes it hard to extract a single univocal legal concept.

[6] Giusella Finocchiaro and Claire Vishik, "Law and Technology: Anonymity and Right to Anonymity in a Connected World," in *Movement-Aware Applications for Sustainable Mobility: Technologies and Approaches*, ed. Monica Wachowicz (IGI Global, 2010), 140-156.

[7] Giusella Finocchiaro, "Anonymity and the law in Italy," in *Lessons from the identity trail*, ed. Ian Kerr, Valerie M. Steeves and Carole Lucock (Oxford University Press, 2009), 523–536.

4.2.2 The Definition of Personal Data

The term "personal data" is defined as follows by Directive 95/46/EC:

> Personal data shall mean any information relating to an identified or identifiable natural person ("data subject"); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.[8]

In the following we focus on three closely interrelated key elements of this definition:

1. "any information";
2. "relating to";
3. "an identified or identifiable".

1. The expression "any information" provides an idea of how wide the notion of personal data is. It is not infrequent to erroneously conceive "personal data" only as information concerning the most intimate aspects of a person. On the contrary, the concept of personal data includes any sort of information about a person, including economic and professional data, and not just data about his/her personal life. Indeed, this expression covers "objective" information, such as job or income as well as "subjective" information, such as opinions or assessments. This concept is also supported by Opinion 4/2007 of Article 29 Data Protection Working Party[9]:

   > Considering the format or the medium on which that information is contained, the concept of personal data includes information available in whatever form, be it alphabetical, numerical, graphical, photographical or acoustic, for example. It includes information kept on paper, as well as information stored in a computer memory by means of binary code, or on a videotape, for instance. In particular, sound and image data qualify as personal data from this point of view, insofar as they may represent information on an individual.

2. In general terms, information can be considered to "relate" to an individual when it is about that individual. In many situations, this relationship can be easily established. For instance, the data registered in a medical record are clearly "related to" an identified patient. Analogously, the image of a person filmed on a video interview is "related to" that person.

   In other situations, however, establishing the relationship between the information and the individual does not come immediately. In order to clarify this point, Article 29 Working Party noted that, "data relates to an individual if it refers to the identity, characteristics or behaviour of an individual or if such information is used to determine or influence the way in which that person is treated or evaluated".[10]

---

[8] Directive 95/46/EC, Art. 2.

[9] Opinion 4/2007 of Article 29 Data Protection Working Party on the concept of personal data, WP 136, 20.06.2007.

[10] Working Party document on data protection issues related to RFID technology, WP 105, 19/01/2005, Art. 8.

3. In general terms, a natural person can be considered "identified" when, within a group of people, he or she is "distinguished" from all other members of the group. Accordingly, the natural person is "identifiable" when, although the person has not yet been identified, it is possible to do so. This means that the subject can be identified through some characteristics or aggregation of data.

   Identification is normally based on particular pieces of information that we may call "identifiers" and which hold a close relationship with the given individual. Examples are outward signs of this person's appearance like height, eye colour, clothing, or a quality of the person that cannot be immediately noticed, like the profession, or the name. We will focus our attention on identifiers in Sect. 4.3.

4.2.3 The Concept of Anonymous Data

The concept of "anonymous data" is not explicitly reported in Directive 96/46/EC. However, this notion can be derived from the definition of "personal data" given in the Directive, and from some Recitals[11] of the same Directive. In particular, Recital no. 26 states that:

> The principle of protection must apply to any information concerning an identified or identifiable individual.

Furthermore:

> […] the principles of protection shall not apply to data rendered anonymous in such a way that the data subject is no longer identifiable.

Further references to "anonymous data" and especially to "anonymization" have been provided in Recitals no. 9, 26, 28 and 33 of Directive 2002/58/EC. In particular, Recital no. 9 states:

> The Member States (…) should cooperate in introducing and developing the relevant technologies where this is necessary to apply the guarantees provided for by this Directive and taking particular account of the objectives of minimising the processing of personal data and of using anonymous or pseudonymous data where possible.

Similarly, Recital no. 30 states that:

> Systems for the provision of electronic communications networks and services should be designed to limit the amount of personal data necessary to a strict minimum (…).

The above Recitals basically state the same principle in different ways: the principle of minimization in data processing. According to this principle, the processing of personal data is permitted only if it is required to achieve a specified purpose: if this very purpose can be accomplished with anonymous or pseudonymous data,

[11] The Recitals are the opening statements that introduce the main provisions of the European Directives and present the reasons for their adoption.

then these latter modalities should be preferred. Given these considerations, we can assume that in Directive 95/46/EC anonymity is considered as the main form of protection of the rights of the subjects whose data are processed.

4.2.4 *A Case Study: The Definition of Anonymous Data in the Italian Personal Protection Code*

Unlike Directive 95/46/EC, the Italian Personal Protection Code (or shortly "the Privacy Code") explicitly defines anonymous data as:

> (…) any data that, in origin or after being processed, cannot be connected to an identified or identifiable person.[12]

The Privacy Code definition has three key elements: the notion of data, the connection between the data and the person, and the identifiability of the latter one. These elements reflect the essential components of the definition of personal data comprised in Directive 95/46/EC.

The data. Briefly, we can assume that the definition of personal data in the Privacy Code, similarly to Directive 95/46/EC, is broad and it includes all information directly or indirectly related to a natural person.[13]

The connection. Both the Privacy Code and Directive 95/46/EC report that an essential element in the definition of anonymous data is the absence of a clear connection between the data and an identified (or identifiable) person. In fact, the distinction between anonymous and personal data actually depends on this connection. One problem is that, according to the definition of personal data given by the Privacy Code, all possible links between a person and information can be considered as personal data, and more subjects can be involved with multiple connections, as shown in Example 1.

Example 1 Consider a report made by a consultant Alice for a banker Bob concerning the financial situation of a client Carl applying for a loan. Alice is author of the report, and this fact is a personal datum related to Alice. Bob is the addressee of the report, and the fact that such a report is addressed to Bob is a personal datum related to Bob. Carl is the person having that financial situation, and the fact that such report concerns his very situation is a personal datum related to Carl. So, here we have three different data subjects, whose connections with personal data can be broken as to create three anonymous data.

---

[12] Italian Personal Protection Code, Legislative Decree no. 196, 30/06/2003, art. 4, co. 1, lett. n).

[13] A recent decision of the Italian Supreme Court (no. 19365, 22/09/2011) has stated the following principle: data about the health of a child is "sensitive data" (according to the definition of Legislative Decree no. 196/2003, art. 4, co. 1, lett. d) of the child's parents: therefore an unlawful processing of this information allows the parents to act for the protection of an own right.

Usually, unlike Example 1, a large amount of data is involved, and the relationship among the entities can be more complex. This example alone, however, highlights that anonymity is a relative and functional concept. In this example, in fact, anonymity would effectively be guaranteed by eliminating the connections between all the three parties involved in the report.

Identifiability. Which criteria should be followed to determine if a subject is identifiable? In Italy, as in other Member States, the evaluation of the measures of identification is carried out accordingly to European legal acts. In particular, Recommendation of the Council of Europe No. R (97) 5[14] specifies whether the impossibility of the connection between information and a person should be absolute or relative. This act states that information cannot be considered identifiable if identification requires an unreasonable amount of time and manpower.

A more accurate investigation of this matter can be found in the Explanatory Memorandum to Recommendation R (97) 18,[15] concerning the protection of personal data collected and processed for statistical purposes. See for instance point No. 52, letter d:

> Conditions for anonymity are relative, especially in relation to the technical means available for identifying data and taking away their anonymity. In this way, in view of the rapid progress in technological and methodological developments, the time and manpower required to identify a person, which would today be considered 'unreasonable', might no longer be so in the future (…).

Example 2 Data concerning "a graduated male living in Milan" would not be considered personal data, since it cannot be linked to a specific person, even if a great amount of time and manpower is used. Vice versa, data referring to "Sergio Mascetti, assistant professor at the University of Milan" should certainly be considered as personal data, since the identification of the person is immediate even with negligible time and manpower. However, it would not be as immediate to evaluate whether data referring to "a graduated male, living in Milan and working for a university, who plays volleyball and is a fan of Bruce Springsteen" should be considered personal data. What is hard to evaluate is how many persons correspond to this description and, even if there is a single one, it is not so clear as to how much time and manpower is required to identify him.

In order to address problems like the one reported in Example 2, it is necessary to analyze each case in its different aspects, taking into account all the following factors, as stated by Opinion 4/2007: the intended purpose of data processing, the way the processing is structured, the advantage expected by the controller, the interests at stake for the individuals, and the risk of organisational dysfunctions and technical

[14] Recommendation No. R (97) 5 of the Committee of Ministers to Member States on the protection of medical data, 13/02/1997.

[15] Recommendation No. R (97) 18 of the Committee of Ministers to Member States on the protection of personal data collected and processed for statistical purposes, 30/09/1997.

failures. The identification process is dynamic and "should consider the state of the art in technology at the time of the processing and the possibilities for development during the period for which the data will be processed".[16]

Observe that in the acts mentioned above the concept of reasonableness is used to assess identifiability. This concept is commonly used in legal systems as a measurement criterion. In this perspective, reasonableness is the criterion used to measure how "easy" it could be to associate a data subject with the data. This approach remarks the fact that anonymity is a relative concept, and its evaluation requires taking into account the particular context at the time of processing.

The degree of anonymity cannot be predetermined: in fact, anonymity may take a different extent depending on the circumstances, among which we may include the will of the data subject. It is therefore essential to suggest some criteria for measuring anonymity. The possible quantification of anonymity will be analyzed from a technological point of view in the next section.

4.3 Anonymity in Data Disclosure

In this section we briefly survey some of the contributions in the Computer Science literature for the problem of guaranteeing anonymity while disclosing data. Note that we have decided to focus our discussion on anonymity models, thereby omitting many other interesting models, such as randomization[17] and differential privacy,[18] whose purpose is to alter the private information, rather than render a data respondent anonymous.

We consider two of the applicative scenarios that have been mainly addressed by the research community: data publication (Sect. 4.3.1) and location based services (Sect. 4.3.2).

4.3.1 Anonymity in Data Publication

As we observed in Sect. 4.2, the disclosure of personal information to the general public or to third parties is subject to the limitations imposed by the regulations on privacy protection. Nevertheless, if this information was rendered anonymous, these

[16] Opinion 4/2007, Art. 12.

[17] Rakesh Agrawal and Ramakrishnan Srikant, "Privacy-preserving data mining," in *Proceedings of the 2000 ACM SIGMOD international conference on Management of data* (New York, NY, USA: ACM, 2000), 439-450.

[18] Cynthia Dwork, "Differential Privacy," in *Automata, Languages and Programming,* 4052:1-12, Springer Berlin/Heidelberg, 2006.

Table 4.1 Hospital database

Name	Gender	Date of birth	ZIP code	Disease
Alice	F	01/01/1981	11111	Flu
Anne	F	02/02/1981	11122	Flu
Sonia	F	12/03/1981	11133	Flu
Bob	M	12/01/1982	33311	Heart disease
Shunsuke	M	10/04/1982	33322	Cold
Carl	M	02/03/1982	33333	Flu

limitations would not apply, hence making it possible to share the information without explicit user agreement and with great benefits both for the entity collecting this information and the other stakeholders. For this applicative reason, the problem of rendering information anonymous before publication has been extensively studied in the scientific literature.[19] In this section we first describe the problem in detail and then survey some of the contributions addressing this problem.

4.3.1.1 Problem Definition and Characterization

The actors involved in a typical data publication scenario are the same described in Sect. 4.2, with the only difference that the controller and the processor are considered as a single entity; for this reason, in the following, when we mention the "controller" we refer to both the controller and the processor. The data flow is the following: the controller collects data from the subjects and wants to release this information to a recipient that can be, for example, a data miner or an analyst. Since we consider that the controller is trusted[20] by the data subject, the overall privacy problem is the following: guaranteeing the data subject's privacy protection, while releasing useful information to the recipient that plays the role of the *adversary*.

Example 1 Consider a hospital (i.e., the data collector) in which patient information (e.g., diseases, therapies, etc.) is collected and stored. Table 4.1 shows an example of this information.

This data is potentially a valuable resource for medical research (i.e., the recipient), but it cannot be disclosed without the user's explicit authorization, due to the regulation in force hence it needs to be altered before disclosure. Figure 4.1 shows a graphical representation of this situation.

[19] Anna Monreale, Dino Pedreschi, and Ruggero G. Pensa, "Anonymity technologies for privacy-preserving data publishing and mining," in *Privacy-Aware Knowledge Discovery: Novel Applications and New Techniques*, F. Bonchi, E. Ferrari, Chapman & Hall/CRC Data Mining and Knowledge Discovery Series, 2010.

[20] Here, the term "trust" is not used here in its proper legal sense but according to its intuitive meaning of "confidence". In this case, it means that the data subject is confident that the data collector will manage his/her data according to the current regulations or to other agreements between the two parties.

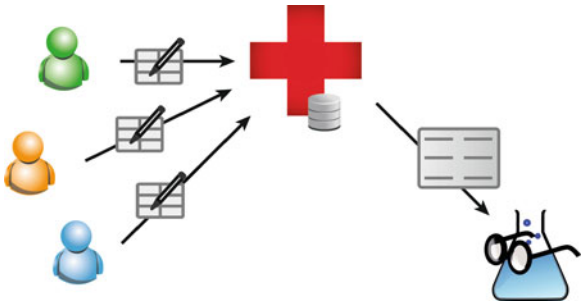


Fig. 4.1 Data flow in the data publication scenario

The problem with protecting data subject privacy when disclosing information is not trivial. Among many others, one intuitive reason is the following: providing data utility and data subject's privacy are contrasting objectives.[21] Indeed, a naïve solution to achieving the best data utility is to provide the recipient with exactly the same information collected by the controller. However, in this case the data subject's privacy is compromised. Vice versa, the best privacy protection is achieved when no data are disclosed, but in this case data utility is null. This is one of the reasons that make the problem scientifically attractive and that have led it to be extensively studied by the Computer Science and the Official Statistics communities. Both communities proposed several mathematical representations of the problem, considering different aspects of it. These mathematical representations, that we call *privacy models*, have two main objectives: to formally describe the problem and to make the correctness of the privacy preserving techniques possible to prove.

Each privacy model defines all the important aspects of the considered problem, like the actors, the flow of data (i.e., collection and successive release), etc. In particular, most of the privacy models defined in the literature identify one aspect that is particularly important: the *attack model*. With this term we indicate the adversary's capabilities used in his attempt to discover the data subject's personal information. These capabilities include the *inference abilities* (i.e., how to derive new information from the existing one) and, in particular, *the background knowledge*, i.e., the information that the recipient owns independently from the data released by the controller. Background knowledge can be originated by several sources, such as well-known facts, demographic information, public records, and information on specific individuals possibly published by the data subject himself (e.g., data published in a social network).

In order to continue with this discussion, it is necessary to better characterize the type of information collected by the controller. Many of the contributions identify four groups of attributes[22] (e.g., each column in Table 4.1 is an attribute):

[21] Tiancheng Li and Ninghui Li, "On the tradeoff between privacy and utility in data publishing," in *Proceedings of the 15th ACM SIGKDD international conference on Knowledge discovery and data mining* (New York, NY, USA: ACM, 2009), 517-526

[22] Valentina Ciriani et al., "Microdata Protection," in *Secure Data Management in Decentralized Systems*, Springer US, 2007, 33:291-321.

- Explicit identifiers of the data subject, such as name and social security number.
- Quasi-Identifiers (QI): attributes that are not explicit identifiers but that, when used in conjunction with background knowledge, can lead the adversary to identify a data subject or to restrict the possible identity of a data subject; the attributes "gender", "ZIP code" and "date of birth" are examples of QI.
- Private Information (PI): personal data that should not be associated to a data subject's identity like, for example, a disease or salary.
- Non-private information: all the attributes that do not fall into the previous categories.

4.3.1.2 *k*-Anonymity

Samarati et al.[23] showed that simply dropping the explicit identifiers does not guarantee anonymity if the adversary knows the population's QI values (this information can be obtained, for example, from the voter list). In this case, referring to Example 1, the adversary can discover that there is a single male person born on the 12/01/1982 who lives at ZIP code 33311. Since this information in the voter list is associated to an explicit identifier (i.e., the name), the adversary can discover that Bob had the flu. This type of attack is sometimes called *record linkage attack.*[24] Typically, a countermeasure against this attack is to apply a transformation to the values in the QI attributes in order to render several records indistinguishable.

A well-known model, defined to contrast the record linkage attack, is *k*-anonymity.[25] This approach became popular in the field of privacy preserving data publication and in many other privacy problems. The idea of *k*-anonymity is to guarantee that information on any data subject cannot be distinguished from the information on other k-1 data subjects. More technically, the privacy requirement defined by *k*-anonymity is that for each record released (e.g., a record is a row in a table) there must be at least other $k-1$ records with the same QI values. The techniques adopted in the literature to enforce *k*-anonymity involve the removal of explicit identifiers and the generalization (e.g., the date of birth is replaced by the year of birth) or suppression (e.g., removing the date of birth) of QI. It is evident that these techniques reduce the accuracy of the disclosed information.

[23] Pierangela Samarati and Latanya Sweeney, "Generalizing data to provide anonymity when disclosing information (abstract)," in *Proceedings of the seventeenth ACM SIGACT-SIGMOD-SIGART symposium on Principles of database systems, PODS '98* (New York, NY, USA: ACM, 1998).

[24] William E. Winkler, *The state of record linkage and current research problems* (Statistical Research Division, U.S. Bureau of the Census, 1999), Washington, DC.

[25] Id. at 17. ("Generalizing data to provide anonymity when disclosing information (abstract)").

Table 4.2 A 3-anonymous version of Table 4.1.

QI attributes			PI attribute
Gender	Date of birth	ZIP code	Disease
F	1981	111*	Flu
F	1981	111*	Flu
F	1981	111*	Flu
M	1982	333*	Heart disease
M	1982	333*	Cold
M	1982	333*	Flu

*denotes that some information has been removed to guarantee anonymity.

Table 4.3 A 3-anonymous table with respect to quasi identifiers QI_1 and QI_2

Gender	Date of birth	ZIP code	Disease
F	1981	333*	Flu
F	1982	111*	Flu
F	1982	111*	Cold
M	1982	111*	Heart disease
M	1981	333*	Cold
M	1981	333*	Flu

*denotes that some information has been removed to guarantee anonymity.

Example 2 Table 4.2 represents a 3-anonymous version of Table 4.1. Note that Table 4.2 reports the year of birth only (instead of the birthdate) and that the last digits of the ZIP Code have been suppressed. In this case, even if the adversary knows the Gender, Date of Birth and ZIP Code of the entire population, he would not be able to distinguish Bob's record from the records of other two users (Shunsuke and Carl).

4.3.1.3 *k*-Anonymity with Multiple QI

Models based on *k*-anonymity assume that the controller knows the QI. However, different adversaries may use different QIs. To address this problem, one extension to *k*-anonymity consists in making multiple QIs possible to specify.[26] In other words, the controller knows a set of quasi-identifiers and the disclosed information has to be k-anonymous with respect to each of them. Example 3 shows that guaranteeing k-anonymity for all the quasi-identifiers in a set Q is not the same as guaranteeing k-anonymity on a QI that is the "union" of all the quasi-identifiers composing Q.

Example 3 Consider the data represented in Table 4.3. Assume that the controller identifies two sets of QI: $QI_1 = \{Gender\}$ and $QI_2 = \{Date\ of\ Birth, ZIP\ Code\}$.

Table 4.3 is 3-anonymo with respect to QI_1 and QI_2, but it is not 3-anonymous when the quasi identifier is $QI_1 \cup QI_2$, i.e., $QI = \{Gender, Date\ of\ Birth, ZIP\ Code\}$. Indeed, there is one group of three records with Gender = "F" and another group of three records with Gender = "M". Similarly, considering QI_2, we can identify two

[26] Benjamin C. M. Fung, Ke Wang, and Philip S. Yu, "Anonymizing Classification Data for Privacy Preservation," *IEEE Trans. on Knowl. and Data Eng.* 19, no. 5 (May 2007): 711–725.

Table 4.4 A 3-anonymous database

Gender	Date of birth	ZIP code	Disease
F	1981	111*	Flu
F	1981	111*	Flu
F	1981	111*	Flu
M	1982	333*	Heart disease
M	1982	333*	Cold
M	1982	333*	Cold

*denotes that some information has been removed to guarantee anonymity.

different groups, each one with three indistinguishable records with respect to the Date of Birth and ZIP Code. However, the table is not 3-anonymous with respect to the set QI = {Gender, Date of Birth, ZIP Code}. For example, there is a single record with the combination Gender = "F", Date of Birth = "1981" and ZIP Code = "333*".

4.3.1.4 *l*-Diversity

The models illustrated in Sects. 4.3.1.2 and 4.3.1.3 aim to avoid that any record in a table can be associated with less than k individuals. However, this property is not sufficient to guarantee an intuitive notion of anonymity. Indeed, it has been shown that, although the adversary may not uniquely identify the data subject "referred" by a record, he can still infer the personal information of that individual. Two attacks have been presented in the literature to achieve this.[27] The former, called "homogeneity attack" is based on a vulnerability of the k-anonymity model and is intuitively explained in the following example.

Example 4 Consider Table 4.2. Suppose that the adversary knows that Alice was born in 1981, lives in the area with ZIP code 11111 and is in the database. He knows that Alice's record is one of the first three in the table. Since all of those patients have the same medical condition (Flu), the adversary can identify Alice's disease.

The latter attack that can be used to violate the data subject's privacy despite k-anonymity, is called "background knowledge attack" since it assumes that the adversary has additional background information. This attack is based on the idea that in some cases there can be a correlation between the QI values and the private information. Consider the following example.

Example 5 Consider the 3-anonymous Table 4.4 and suppose that the adversary knows that Shunsuke is in the database, was born in 1982 and is Japanese.

The attacker can infer that Shunsuke's record is one of the last three records in the above table. Also, by knowing that Japanese people have a low incidence of heart disease, the adversary can conclude with high likelihood that Shunsuke has a Cold.

[27] Ashwin Machanavajjhala et al., "l-diversity: Privacy beyond k-anonymity," *ACM Trans. Knowl. Discov. Data* 1, no. 1 (March 2007): 24.

Table 4.5 A database satisfying 3-diversity

Gender	Date of birth	ZIP code	Disease
F	1981	111*	Flu
F	1981	111*	Cancer
F	1981	111*	Cold
M	1982	333*	Heart disease
M	1982	333*	Flu
M	1982	333*	Cold

It is worthwhile observing that there is a significant conceptual difference between the two attacks above. The former (i.e.: the "homogeneity attack") takes place under the same assumptions specified for *k*-anonymity and exploits a vulnerability of this model. Vice versa, the latter (i.e.: the "background knowledge attack") exploits some background knowledge that the *k*-anonymity model assumes as not available to the attacker. Note that, in general, given a privacy preserving technique that is safe under a privacy model, it is always possible to find a counter example to show that that technique is insufficient (or "unsafe") by using more background knowledge than assumed in that privacy model.

The *l-diversity* model was proposed in order to overcome the weakness of *k*-anonymity and to counter the two attacks illustrated above.[28] The aim is to obtain groups of data subjects with indistinguishable QIs and an acceptable diversity of the attributes' values representing personal information. In particular, the main idea of this method is that every k-anonymous group should contain at least *l* values for the attributes containing personal information. Different instantiations of the *l*-diversity definition have been presented by Machanavajjhala et al.[29] and Xiao et al.[30]

Example 6 Consider the database represented in Table 4.5. It satisfies 3-diversity and it is safe against the attacks illustrated in Examples 4 and 5. Indeed, the adversary cannot understand if Alice suffers from "Flu", "Cancer" or "Cold". Moreover, when the adversary tries to identify Shunsuke's disease, after excluding "Heart Disease", there are still two other possible diseases.

4.3.1.5 *t*-Closeness

It has been observed that in some cases the *l*-diversity model can lead to unnecessary generalization, if we consider different degrees of "sensitivity" of private information. This is better explained by the following example.

[28] Id. at 21 ("l-diversity: privacy beyond k-anonymity").

[29] Id.

[30] Xiaokui Xiao and Yufei Tao, "Personalized privacy preservation," in *Proceedings of the 2006 ACM SIGMOD international conference on Management of data*, SIGMOD '06 (New York, NY, USA: ACM, 2006), 229–240.

Table 4.6 A k-anonymous database

Age	ZIP code	Disease
[21–30]	111*	Negative
[21–30]	111*	Negative
[21–30]	111*	Negative
[21–30]	111*	Negative
[41–45]	222*	Negative
[41–45]	222*	Positive
[41–45]	222*	Negative
[41–45]	222*	Positive
[31–40]	111*	Positive
[31–40]	111*	Positive
[31–40]	111*	Positive
[31–40]	111*	Negative
…		
[60–70]	444*	Negative

*denotes that some information has been removed to guarantee anonymity.

Example 7 Consider the data in Table 4.6 where the attribute "Disease" contains the value "Negative" for patients with a negative HIV test result and the value "Positive" for those with a positive test result. Assume that in this table we have 10,000 records and only 1% of them has Disease = "Positive". Clearly, the two values have a different degree of sensitivity. Intuitively, a patient with a negative test result would not mind the result being known, because it is the same as that of 99% of the population, but he/she would not want to disclose a positive value. Therefore, the level of anonymity required for the first group in Table 4.6 (i.e., age "[21–30]", ZIP code "111*") is intuitively weaker than the one required for the second group (age [41–45], ZIP code "222*").

Another problem with *l*-diversity is that it can be insufficient to prevent the disclosure of private information when the adversary knows the distribution of the private values. Indeed, if the adversary has prior knowledge about private information on a data subject, he can compare this knowledge with the probability computed from observing the disclosed information. In Example 7, the adversary knows that the average distribution of positive HIV persons is 1%. After observing the disclosed information, the adversary discovers that Bob (age 32 and living in ZIP code 11123) has a much higher probability to be HIV positive (i.e., 75%).

In order to avoid the above weakness of *l*-diversity, Li et al. introduced the *t*-closeness model.[31] This technique requires that in any group of QIs the distribution of the values of an attribute containing personal information is close to the distribution of the attribute values in the overall table. The distance between the two distributions should be no more than a threshold *t*. Clearly, this limits the information gained by the adversary after an attack.

[31] Ninghui Li, Tiancheng Li, and S. Venkatasubramanian, "*t*-closeness: Privacy Beyond k-Anonymity and l-Diversity," in *Data Engineering, 2007. ICDE 2007. IEEE 23rd International Conference on*, (Istanbul, Turkey: IEEE Computer Society, 2007) 106–115.

4.3.2 Anonymity When Disclosing Spatio-Temporal Information

So far, most of the techniques illustrated in this section assume that the data to disclose are either in the form of numbers (e.g., the age, the salary, etc.) or elements organized in taxonomy (e.g., gender, diseases, etc.). Several contributions investigate the problem of guaranteeing users' anonymity in presence of spatio-temporal information. We first describe the problem (Sect. 4.3.2.1) and then introduce the models and techniques proposed in the Computer Science literature to address it (Sect. 4.3.2.2).

4.3.2.1 Problem Description

Some preliminary contributions motivate that specialized techniques are required in presence of spatio-temporal information,[32,33] This is mainly due to three reasons. First, it is commonly recognized that this kind of information has a very specific semantic that calls for specialized data managements methods. Secondly, most of the techniques related to data publication (like the ones introduced in Sect. 4.3.1) assume that each data subject is associated with a fixed amount of information (e.g., a single record), while many of the applications that involve spatio-temporal information associate a list of locations (also called a "trace") with each user. The last, but conceptually most important reason, is that in many practical cases, space and time can have the double role of quasi identifiers and of private information (see Example 8 below).

Spatio-temporal information is particularly relevant from an applicative point of view, because it is the fundamental data type in geo-referenced applications and services that are becoming popular mainly thanks to the diffusion of mobile devices (e.g., smartphones). These devices are "location-aware" in the sense that they are equipped with hardware peripherals that make their geographical location possible to detect. This new feature gives raise to a new class of Internet services, called *Location Based Services* (LBS), in which one of the parameters of the requests is the current location of the user. One example of LBS is the "find the closest Point of Interest (POI)" where a POI is, for instance, a restaurant. In this context, privacy should be safeguarded both when each request is issued (this is sometimes called the "on-line" privacy protection problem) and when a dataset of formerly acquired location information needs to be disclosed (i.e., the "off-line" privacy protection problem).

The actors in this scenario are similar to the ones in the data publication scenario. In the "off-line" privacy protection problem the *user* (i.e., the data subject) reports

[32] Marco Gruteser and Dirk Grunwald, "Anonymous Usage of Location-Based Services Through Spatial and Temporal Cloaking," in *Proceedings of the 1st international conference on Mobile systems, applications and services*, MobiSys '03 (New York, NY, USA: ACM, 2003), 31–42.

[33] Sergio Mascetti et al., "k-Anonymity in Databases with Timestamped Data," *in Proceedings of the Thirteenth International Symposium on Temporal Representation and Reasoning* (Washington, DC, USA: IEEE Computer Society, 2006), 177–186.

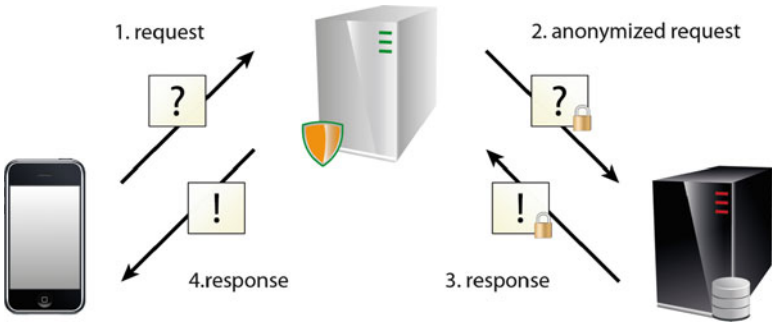


Fig. 4.2 Data flow in the provisioning of a LBS service with anonymization

Fig. 4.3 (**a**) *On the left*, reported users' locations. (**b**) *On the right*, identification of commonly visited places

his/her locations to a trusted *location server* (i.e., the controller and processor) that collects the information. After proper modifications, the location server discloses the location information to a third party (i.e., the recipient), which is not trusted by the user. On the contrary, in the "on-line" privacy protection problem the user communicates with the *service provider* that is not trusted by the user, thereby playing the role of the recipient. In this case, the role of controller and processor is played by a trusted entity, called *anonymizer*, which is in charge of enforcing the user's anonymity. As shown in Fig. 4.2, a user issues a LBS request to the anonymizer, that properly modifies and forwards it to the service provider. The anonymizer also forwards the reply from the service provider to the user.

Example 8 Let's consider an LBS in which an "anonymous" user frequently reports his/her location (see Fig. 4.3a). By observing this information, the service provider can identify two recurring places from which most of the requests are issued (see Fig. 4.3b). The temporal information indicates that the reports from one of these two places occur during working hours, while the ones from the other place occur during non-working hours. Given this analysis, the service provider can conclude,

Fig. 4.4 Example of location 3-anonymity

with high likelihood, that the two places are the user's home and work place. From public sources, like a phone book, the service provider can compute the set of people living in that home address and working in that workplace. If the intersection of these two sets contains one person, the adversary can re-identify the user. Moreover, from the analysis of the reported locations, the service provider can also observe that there are other usual places for that user. One of these places is a Church, from which the user generally reports locations on Sunday morning. Given this observation, the service provider can deduce, with high likelihood, the user's religious belief.

4.3.2.2 Privacy Models for LBS Anonymity

The core idea of the defence techniques based on anonymity is to alter each request so that the exact location is transformed into a "generalized region" in such a way that an adversary cannot identify the possible issuer in a set that contains at least k users (see Example 9).

Example 9 Consider Fig. 4.4. The position labelled "A" is the current location of Alice, who is issuing an LBS request. The other markers represent the location of other four users. Assume that the adversary's background knowledge includes the identities and the corresponding positions of all five persons. Even if Alice removes any of the explicit identifiers from the LBS request, the adversary can re-identify her if Alice's exact location is reported. Vice versa, if the location of Alice is generalized to the dark-grey rectangle represented in Fig. 4.4 before the request is sent to the service provider, the adversary cannot identify the issuer of the request in the set of three persons, hence guaranteeing a form of 3-anonymity to Alice.

It is important to observe that the attack illustrated in Example 9 requires the adversary to have background knowledge that associates each user's location with the identity of that user. One problem is modelling how much information the adversary has. Indeed, on one hand, there is a common agreement about the fact that an adversary can partially obtain this background knowledge like, for example, the

information exploited by the adversary in Example 9. On the other hand, the adversary is unlikely to have "full background location knowledge", i.e., to know the location of each person in each time instant. In other words, the adversary has "partial background location knowledge" and the problem is how to model it.

In order to tackle this problem, a common approach is to assume that the anonymizer ignores the background information available to the adversary. In this case, it is assumed that the adversary always has "full background location knowledge". This is a "conservative" approach in the sense that if a defence technique is proved as safe under this assumption, it can be proved as safe in any case of partial background knowledge,[34,35,36,37] The drawback of this approach is that, by assuming "full background location knowledge", the anonymizer needs to generate large generalized regions that may render the service impractical. Some papers tackle this problem by assuming that the anonymizer can estimate an upper bound for the background knowledge available to the adversary and this bound is less than the "full background location knowledge". The advantage of the techniques proposed under this assumption is that the generalized region, required to achieve anonymity, is generally smaller,[38,39] However, the problem with this approach is that if the assumption about the adversary knowledge is incorrect, and the adversary actually has more background knowledge than assumed, then there are no guarantees on the actual anonymity of the disclosed information.

The first paper addressing the problem of guaranteeing *k*-anonymity when providing an LBS service considers an adversary with "full background location knowledge".[40] Although on one side this model is conservative, it has been shown that, from other perspectives, this model is not sufficiently conservative, leading to possible privacy breaches. Two formal models independently proposed by Kalnis et al.[41] and Mascetti et al.[42] capture this problem. The intuition is the following: the attack

[34] Id. at 29 ("Anonymous Usage of Location-Based Services Through Spatial and Temporal Cloaking").

[35] Mohamed F. Mokbel, Chi-Yin Chow, and Walid G. Aref, "The new Casper: query processing for location services without compromising privacy," in *Proceedings of the 32nd international conference on Very large data bases*, VLDB '06 (Seoul, Korea: VLDB Endowment, 2006), 763–774.

[36] Panos Kalnis et al., "Preventing Location-Based Identity Inference in Anonymous Spatial Queries," *IEEE Trans. on Knowl. and Data Eng.* 19, no. 12 (December 2007): 1719–1733.

[37] Sergio Mascetti et al., "Spatial generalisation algorithms for LBS privacy preservation," *J. Locat. Based Serv. 1*, no. 3 (September 2007): 179–207.

[38] Claudio Bettini et al., "Anonymity in Location-Based Services: Towards a General Framework," in *Proceedings of the 2007 International Conference on Mobile Data Management* (Washington, DC, USA: IEEE Computer Society, 2007), 69–76.

[39] Manolis Terrovitis and Nikos Mamoulis, "Privacy Preservation in the Publication of Trajectories," in *Proceedings of the Ninth International Conference on Mobile Data Management* (Washington, DC, USA: IEEE Computer Society, 2008), 65–72.

[40] Id. at 29 ("Anonymous Usage of Location-Based Services Through Spatial and Temporal Cloaking").

[41] Id at 35 ("Anonymity in Location-Based Services: Towards a General Framework").

[42] Id. at 36 ("Privacy Preservation in the Publication of Trajectories").

Fig. 4.5 Failure of location anonymity in the "historical case"

model considered by Gruteser et al. implicitly assumes that the adversary does not know the defence technique. If this assumption does not hold, which is often the case, the defence technique proposed by Gruteser et al. may fail to provide the required level of anonymity.

Another limit of some existing models,[43,44,45,46] is assuming that the adversary cannot associate two or more requests with the same user. This assumption is sometimes called the "snapshot case" since it is equivalent to assuming that the adversary can observe the users' positions and requests in a given instant and cannot "follow" the users' movements. However, in many practical cases, each user is associated with a pseudo-id (a unique value, whose association with the real user identity is kept secret) that is sent by the user with each request. In this "historical case" the adversary can understand that a single user issues two or more requests. It has been shown that this knowledge may render ineffective the defence techniques proposed for the "snapshot case" (see Example 10). This problem has been addressed, among others, by Bettini et al.[47] and Riboni et al.[48]

Example 10 Consider Fig. 4.5 that represents the locations of five users in two different time instants. Alice is the user labelled "A" who issues two LBS requests, one in each time instant. According to the intuitive definition of *k*-anonymity provided above, the two dark-grey rectangles reported in the figure guarantee a form of

[43] Id. at 29 ("Anonymous Usage of Location-Based Services Through Spatial and Temporal Cloaking").

[44] Id. at 32 ("The new Casper: query processing for location services without compromising privacy").

[45] Id. at 35.

[46] Id. at 36.

[47] Claudio Bettini, "Privacy and anonymity in Location Data Management," in *Privacy-Aware Knowledge Discovery: Novel Applications and New Techniques*, ed. F. Bonchi, E. Ferrari, Chapman & Hall/CRC Data Mining and Knowledge Discovery Series, 2010.

[48] Daniele Riboni et al., "Preserving Anonymity of Recurrent Location-Based Queries," in *Proceedings of the 2009 16th International Symposium on Temporal Representation and Reasoning*, TIME '09 (Washington, DC, USA: IEEE Computer Society, 2009), 62–69.

3-anonymity. However, if the adversary is able to understand that a single user issued both requests, the only possible issuer is Alice since she is the only user that is located within both rectangles.

4.4 Discussion

In this section lawyers and computer scientists "talk to each other". After the analysis of the anonymity concept, conducted in accordance with traditional approaches in both areas, we now highlight the main similarities and differences between the Legal and Computer Science fields. We argue that a "neutral" study of the two approaches is necessary to obtain a complete picture of the problem. This result should then be used as a starting point for innovative research in the area of privacy protection. We do not assume that one or the other approach is wrong or entails unsolvable problems and that it should, consequently, be changed and adapted to the other. By putting aprioristic statements aside, we aim to analyze both approaches under the same perspective, which is based on a systematic examination of the problem, starting with a detailed linguistic and formal analysis.

4.4.1 The Role of Anonymity in Privacy Preservation

As observed in Sect. 4.2, the legal notion of anonymity, as defined in the legislation on data protection, cannot be seen as a right in itself. Instead, anonymity should be considered as a "tool" that can be used to safeguard the protection of personal data. This interpretation is compatible with the current approach adopted in Computer Science. Indeed, although most of the scientific contributions tackle the problem of guaranteeing privacy through anonymity, it has also been recognized that privacy protection can also be achieved without anonymity. Consider the following example.

Example 11 Assume a geo-referenced social network in which each user can share his/her location with some friends. Note that, if we address the privacy problem of a user Alice with respect to her friend Bob (i.e., Bob is the adversary), anonymity cannot be used to protect privacy, since the service requires Bob to know which user is located in a given location. Also, pseudonyms are not effective, since in many cases Bob knows Alice in person. One solution that Alice can adopt to protect her privacy is to avoid using the service or to exclude Bob from the list of users enabled to see her location. However, the question is whether it is possible to allow Alice and Bob to enjoy the service, while still providing a form of privacy protection. One solution is to allow Alice to specify her "privacy preference" in terms of an "obfuscated area": Bob will only be able to understand that Alice is in that area, and the adopted technique ensures that Bob cannot understand where Alice is located within

Fig. 4.6 Two examples of "obfuscated area"

that area. Figure 4.6 shows Alice's actual position (that is hidden from Bob) and two possible "obfuscated areas" (the dark-grey rectangles), the larger one providing a higher level of privacy protection.

As shown in Example 11, when it is not possible or convenient to render the data anonymous, one approach is to allow each user to specify which information is "sensitive" (accordingly to the will of the data subject) and to guarantee that only "non-sensitive" information is disclosed. Determining whether these techniques are supported by sound legal bases is out of the scope of this paper, but it certainly is an interesting research topic. Indeed, from a legal point of view, the problem cannot be easily solved. The law's requirement, in a general sense, is to protect the fundamental rights of the individuals, giving equal importance to all information, without any difference in value. In particular, the issues concerning the possibility of allowing each data subject to choose the preferred level of privacy have still not been extensively addressed in European directives.

4.4.2 Identifying Information and Personal Data

Another point in common between Law and Computer Science is that both recognize the relative nature of anonymity. In particular, the intuition that simply dropping explicit identifiers is not sufficient to guarantee anonymity is formulated in the legal context (e.g., see Sect. 4.2.3) and it is also supported by formal models presented in the scientific literature (among the others, in Samarati et al.[49] and Gruteser et al.[50]). Indeed, although legal norms do not explicitly distinguish between "explicit identifiers" and "quasi identifiers", this distinction is compatible with the current legal approach.

[49] Id. at 17 ("Generalizing data to provide anonymity when disclosing information (abstract)").

[50] Id. at 29 ("Anonymous Usage of Location-Based Services Through Spatial and Temporal Cloaking").

Vice versa, the specification of "personal" (or "private") information is different in the two areas of Law and Computer Science. Indeed, as explained in Sect. 4.2.2, the term "personal data" denotes any kind of information about a person, including information that is intuitively "sensitive" (like religious beliefs) and those that are not (like eyes colour). Also, the term "personal data", as intended in legal norms, refers both to information that should only be known by a given entity (like health status or the number of requests issued to a given LBS) and to data that can easily be found in external sources (e.g., the home address) and that, hence, can possibly be used to re-identify a subject. In contrast, the term "private information" specified in the Computer Science literature only refers to information that, intuitively, users are not willing to disclose. So, we can identify two differences:

1. The concept of "non-private attributes", formulated in Computer Science, does not have a counterpart in the legal notion.
2. Private information, as defined in Computer Science, does not include quasi-identifiers while, according to legal definitions, quasi-identifiers are actually considered as personal information.[51]

The consequence of problem (1) is that it can contribute to rendering the solutions proposed in Computer Science not adhering to the legal norm, with a consequent impact, as we shall see in the following, on the applicability and usefulness of the Computer Science solutions.

Probably, one of the reasons that lead to difference (2) is that, from the Computer Science point of view, when the anonymization problem is addressed, it is not necessary to avoid the disclosure of quasi-identifiers since, by definition, the adversary can externally find this information in association with the user's explicit identifier. In practice, it is assumed that if a datum is publicly available, then its re-publication does not violate the subject's privacy. However, this approach does not take into account that from the legal point of view (e.g., in the Italian legal system), even if a datum is already public, it cannot be freely processed, but only be used for the purpose for which it was made public. For example, if personal data on Alice are published in the voters' list, this information cannot be published by a web service for marketing purposes even if there is no additional data associated with Alice's record, unless Alice gives her explicit authorization. In other words, it could be misleading to qualify a datum as "public" because a published datum is not always free from legal constraints. One of the reasons behind this difference is that the concept of "purpose of data processing", which has an important role from the legal point of view, is neglected in Computer Science.

It is worthwhile to wonder whether it is possible to fix the two problems above. For what concerns problem (1), there is an easy way out that consists in assuming that, in each application of the privacy models, the set of "non-private attributes" is empty. The solution to problem (2) is more complicated. Consider the following example.

[51] It is worthwhile to note that some papers that have recently appeared in the computer science literature do not distinguish between quasi-identifiers and personal information. Among others, the paper: Arvind Narayanan and Vitaly Shmatikov, "Robust De-anonymization of Large Sparse Datasets," *IEEE Symposium on Security and Privacy*, 0 (2008): 111-125.

Example 12 In this example we refer to the data reported in Table 4.5. According to the definitions provided in the Computer Science literature, assume that the attributes "Gender", "Date of Birth" and "ZIP Code" are quasi identifiers, while "Disease" is private information. According to the definition of *l*-diversity, the table satisfies the 3-diversity property. However, observe that, if an adversary knows that Alice is one of the subjects in this table, he can discover her year of birth and three digits of her ZIP code (since all women in the dataset have the same values for these attributes). The question is: should the publication of this table (without the explicit user's authorization) be considered a privacy violation? The aim of the models provided in Computer Science is to give an ultimate answer to this question: once a model is defined, it is possible to automatically evaluate whether anonymized information can be published or not. On the other hand, from the legal point of view, a unique answer cannot be provided. It is necessary to take into account the purpose of the publication, the compliance with legal constraints (and the legal constraints differ from one country to another) and the nature of the controller (public or private).

Example 12 shows that, although Table 4.5 satisfies the privacy requirements defined by a privacy model, the disclosure of the table may still be considered non-compliant with the regulations. In other words, the model fails to define when the disclosure does not violate the data respondents' privacy. The technical reason does not lie in a particular problem of the *l*-diversity model, but in a transversal problem that affects most of the privacy models proposed in the literature and in particular their relation to the legal norms. Indeed, some pieces of information can actually be disclosed to those adversaries that have less information than assumed. Consider once again Example 6: an adversary that knows, for each of the subjects in the table, the values of the subject's quasi-identifiers, cannot learn any information from the disclosure of Table 4.5. Vice versa, if an adversary does not know Alice's age, but only that Alice is in that table, he can discover her age. This has an impact on the possibility to disclose Table 4.5. Indeed, despite the fact that Alice's age could be discovered from other sources, according to existing regulations, this datum cannot be freely disclosed.

Technically, a defence technique to contrast the above problem requires to apply an idea similar to the one proposed by Fung[52] (see Sect. 4.3.1.3) that makes it possible to model different quasi identifiers. In practice, instead of considering a single set of quasi-identifying attributes, like in the *l*-diversity model, it would be necessary to model as QI each possible combination of "quasi-identifying attributes". Clearly, it should be investigated whether this approach is practical or not in terms of generalized data quality.

4.4.3 Anonymity Measurement

Another difference between the Legal and Computer Science fields concerns how to evaluate whether an individual is identifiable or not. Note that this topic is of paramount

[52] Id. at 20 ("Anonymizing Classification Data for Privacy Preservation").

importance, since it is needed to evaluate whether data are actually anonymous or can be re-associated with a specific individual.

To the best of our knowledge, one of the main legal references to this problem suggests to measure the difficulty in re-identifying the data subject in terms of "time and manpower".[53] This definition is suitable for traditional computer security problems. For example, the difficulty to decrypt a message without the proper key can be measured in terms of how long would it take to try all possible keys i.e., the so called "brute force" attack. However, the question is: does the same measure apply to the problem of guaranteeing privacy? As shown in Sect. 4.3, all the formal models proposed in the Computer Science literature indicate that the key factor affecting the difficulty to re-identify an anonymous datum is the background knowledge available to the adversary, while the adversary's manpower and time to perform the attack are not relevant parameters. Consider, for instance, Table 4.4 in Example 5. Even if the adversary has almost infinite resources (computational power, time and manpower), it would not be possible to identify Shunsuke's data record to infer his disease without additional information. Vice versa, if the adversary knows a piece of background knowledge as in Example 5, i.e., Shunsuke is in the database, was born in 1982 and is Japanese, then it is easy to immediately infer that Shunsuke has a cold, even with negligible computational power, time and economic resources.

According to the above consideration, it seems more reasonable that "time and manpower" should not be adopted to directly measure the effort required to violate anonymity but that, instead, they should measure the effort required by the adversary to acquire background information that in turn can be used to re-identify a data subject. For example, the knowledge of the adult individuals living in a certain area, together with some personal information (e.g., date of birth, home address, etc.…) should be considered as "reasonably" available information for any adversary, since this information is contained in the voters list that in many countries can be obtained for free or at a small price. Vice versa, the "full background location knowledge" (see Sect. 4.3.2.2) could be obtained by physically spying a set of persons or, with some additional approximation, by violating the information system of mobile phone operators, hence acquiring the traces of movements of a large number of users. Both solutions for acquiring the "full background location knowledge" would probably be considered as "unreasonably costly".

It would therefore be desirable, under the legal point of view, to clarify the notion of reasonableness, taken as a measurement criterion of time, cost and resources. We believe that this clarification should be one of the main purposes of the next reform of the European Directive on personal data protection. In this respect, we suggest that reasonableness should be intended as "reasonableness of knowledge" by third parties of information and criteria for the identification of subjects.

[53] Id. at 13 ("Recommendation No. R (97) 5 on the protection of medical data").

4.4.4 Anonymity and the Principle of Minimization

According to the principle of minimization, personal data processing is allowed only for the achievement of a specified purpose and, if this task can be accomplished with anonymous or pseudonymous data, this form of information should be preferred. The objective of this principle is to promote the use of anonymous or pseudonymous data when possible. However, as we shall see in the following, some technical problems arise in the application of this principle.

In many cases transforming data to achieve anonymity causes information loss, and this can make the result of the subsequent analysis approximate. Consider for instance a research centre that wants to know the date of birth of the users for each ZIP code value. If this query is performed using the exact data (e.g., Table 4.1), the answer contains the exact dates of birth. In contrast, if the query is performed on the data in Table 4.2, the research centre can only know the year of birth. Clearly, the result of the query in this last case is less accurate, but in some contexts it could be acceptable if, at the same time, it does not reveal the data subject's personal information.

The problem here is the following: the process of rendering the information anonymous, as commonly intended in the Computer Science literature, necessarily involves a form of data suppression and/or generalization. This implies that the resulting information is less accurate than the original one. Consequently, in many cases, the anonymous version of the information makes it impossible to achieve exactly the same results that would be achieved with non-anonymous data, hence motivating the disclosure of the non-anonymous information. In other words, since the principle of minimization does not take into account any form of approximation in the result, it can be used as a motivation for a controller not to release anonymous data, which is conceptually opposes the core idea behind the principle of minimization.

One final observation: the minimization principle is general and, in itself, must be shaped case by case. Indeed there may be situations in which the value of information plays a predominant role with respect to its "confidentiality". However, this does not apply in general. Perhaps a specification of this principle, or simply a reinterpretation of this principle, in light of the standard of reasonableness, would enhance its practical applicability.

4.5 Conclusions and Future Work

In this paper we addressed the topic of anonymity as a tool to protect personal privacy. The overall objective was to encourage the discussion between Law and Computer Science experts on a topic that is bound to be subject of research in the next years. To achieve this, we presented a brief analysis of the state of the art of this problem from the two points of view. Despite the different methodological

approaches, the challenge was to identify a common language for general definitions. This highlighted the fact that some notions commonly adopted in the Computer Science literature do not find any legal support. Analogously, some legal definitions seem to ignore conceptual issues that are clearly identified in the formal models proposed in Computer Science research. Overall, this paper identifies a few common aspects and several differences between the definitions and results suggested in the two disciplines.

In particular, we observed that the notion of anonymity has a central role both in regulations on personal data protection and in the techniques proposed to protect subject's privacy. Indeed, the anonymity measures proposed in the Computer Science field, support the fact that anonymity is a relative notion that depends on the context. On the other hand, Computer Science has shown the limits of anonymity, hence posing new juridical questions about its role. Despite this point in common, an agreement is missing on some of the basic concepts related to anonymity, like the notion of quasi-identifiers and personal data. This poses new challenges to researchers in both communities. Similarly, according to the state of the art in the two areas, it is still unclear how to measure the "level of anonymity" of a datum. If the interpretation of European legislation suggested in Sect. 4.4 is accepted, and the problem is clarified under the legal point of view, it will be necessary to identify the most suitable formal models to practically compute the measure. Finally, we considered the principle of minimization, showing how its current formulation can motivate the processing and disclosure of identified information, in contrast with the overall idea of this principle.

This paper poses the basis for a new approach to the analysis of the personal data protection problem, suggesting a number of new challenges and research directions.

First of all we plan to extend research to the general problem of privacy protection beyond anonymity. Indeed, there are some concepts that need to be investigated, including the legal foundations of the "obfuscation" functions (see Sect. 4.4.1) and the involved privacy "negotiation" between the controller and subject. Another topic, which is becoming popular in the Computer Science community, is the notion of "differential privacy": it would be of great interest to analyze this concept from the legal point of view, making an effort to identify whether it is compliant with the law. Moreover, it could be interesting to analyse the anonymity problem in "credential systems" in which each user is identified by a different pseudonym by different organizations. The challenge is to prevent the possibility to link different pseudonyms.[54]

Another research effort should be devoted to analyzing the existing privacy protection tools available in commercial applications and services. Indeed, in absence of consolidated technical solutions based on sound legal bases, business companies are addressing the personal data protection problem with ad hoc solutions, and in some case it can be unclear which are the technical or legal fundamentals of these techniques.[55]

[54] David Chaum, "Showing credentials without identification transferring signatures between unconditionally unlinkable pseudonyms," in *Advances in Cryptology - AUSCRYPT '90*, 453:245-264, Springer Berlin/Heidelberg, 1990.

[55] This problem can also be focused in the discussion about on the notion of "accountability".

Considering the privacy problem from a practical point of view, the topic of privacy preservation in social networks would definitively deserve a thorough investigation with the interdisciplinary methodology adopted in this paper. Indeed, although it has already been recognized that specialized techniques are required for these specific services, it is still unclear whether the existing norms can be adapted to this context. For example, one problem is that each data subject can publish information about other users, hence playing the role of the controller. In general, these services involve at the same time categories of subjects having different roles with respect to the processing of data, and it is unclear whether these subjects are captured by existing legal norms. Vice versa, it is necessary to have a clear mapping of the roles involved in the data processing and of the connected liabilities.

As we observed, there are several open issues that need to be addressed. Consequently, it is necessary to continue and enhance the dialogue between researchers in the Law and Computer Science communities, in order to allow the possibility of satisfying the need to balance the use of advanced technologies with the protection of individual fundamental rights. The necessity to develop shared solutions to this problem is part of a process that cannot be anything but interdisciplinary. Indeed, without a practical approach, the risk is that Law becomes hardly applicable. Analogously, Computer Science risks to be a dead end if it is not modelled according to the regulations in force.

References

Agrawal, Rakesh, and Ramakrishnan Srikant. 2000. Privacy-preserving data mining. In *Proceedings of the 2000 ACM SIGMOD international conference on management of data*, 439–450. New York: ACM.

Bettini, Claudio. 2010. Privacy and anonymity in location data management. In *Privacy-aware knowledge discovery: Novel applications and new techniques*, ed. F. Bonchi and E. Ferrari. Boca Raton: Chapman & Hall/CRC Data Mining and Knowledge Discovery Series.

Bettini, Claudio, Sergio Mascetti, X. Sean Wang, and Sushil Jajodia. 2007. Anonymity in location-based services: Towards a general framework. In *Proceedings of the 2007 international conference on mobile data management*, 69–76. Washington, DC: IEEE Computer Society.

Chaum, David. 1990. Showing credentials without identification transferring signatures between unconditionally unlinkable pseudonyms. In *Advances in Cryptology – AUSCRYPT '90*, ed. J. Seberry, J. Pieprzyk, 453:245–264. Berlin/Heidelberg: Springer.

Ciriani, Valentina, Sabrina di Vimercati, Sara Foresti, and Pierangela Samarati. 2007. Microdata protection. In *Secure data management in decentralized systems*, vol. 33, ed. Yu Ting and Sushil Jajodia, 291–321. New York: Springer.

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281, 23.11.1995, 31–50.

Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), OJ L 201, 31.7.2002, 37–47.

Dwork, Cynthia. 2006. Differential privacy. In *Automata, languages and programming*, 4052:1–12, ed. Michele Bugliesi, Bart Preneel, Vladimiro Sassone, and Ingo Wegener. Berlin/Heidelberg: Springer.

Finocchiaro, Giusella. 2009. Anonymity and the law in Italy. In *Movement-aware applications for sustainable mobility: Technologies and approaches*, ed. Ian Kerr, Valerie M. Steeves, and Carole Lucock, 523–536. Oxford: Oxford University Press.

Finocchiaro, Giusella, and Claire Vishik. 2010. Law and technology: Anonymity and right to anonymity in a connected world. In *Movement-aware applications for sustainable mobility: Technologies and approaches*, ed. Monica Wachowicz, 140–156. Hershey: IGI Global.

Fung, Benjamin C.M., Ke Wang, and Philip S. Yu. May 2007. Anonymizing classification data for privacy preservation. *IEEE Transactions on Knowledge and Data Engineering* 19(5): 711–725.

Gruteser, Marco, and Dirk Grunwald. 2003. Anonymous usage of location-based services through spatial and temporal cloaking. In *Proceedings of the 1st international conference on mobile systems, applications and services*, 31–42. MobiSys '03. New York: ACM.

Italian Personal Protection Code, Legislative Decree no. 196, 30/06/2003, art. 4, co. 1, lett. n.

Kalnis, Panos, Gabriel Ghinita, Kyriakos Mouratidis, and Dimitris Papadias. December 2007. Preventing location-based identity inference in anonymous spatial queries. *IEEE Transactions on Knowledge and Data Engineering* 19(12): 1719–1733.

Li, Tiancheng, and Ninghui Li. 2009. On the tradeoff between privacy and utility in data publishing. In *Proceedings of the 15th ACM SIGKDD international conference on knowledge discovery and data mining*, 517–526. New York: ACM.

Li, Ninghui, Tiancheng Li, and S. Venkatasubramanian. 2007. *t*-closeness: Privacy beyond *k*-anonymity and *l*-diversity. In *IEEE 23rd international conference on data engineering, 2007* (*ICDE 2007*), 106–115. Istanbul, Turkey: IEEE Computer Society.

Machanavajjhala, Ashwin, Daniel Kifer, Johannes Gehrke, and Muthuramakrishnan Venkitasubramaniam. March 2007. *l*-diversity: Privacy beyond *k*-anonymity. *ACM Transactions on Knowledge Discovery from Data* 1(1): 24.

Mascetti, Sergio, Claudio Bettini, X. Sean Wang, and Sushil Jajodia. 2006. *k*-anonymity in databases with timestamped data. In *Proceedings of the thirteenth international symposium on temporal representation and reasoning*, 177–186. Washington, DC: IEEE Computer Society.

Mascetti, Sergio, Claudio Bettini, Dario Freni, and X. Sean Wang. September 2007. Spatial generalisation algorithms for LBS privacy preservation. *Journal of Location Based Services* 1(3): 179–207.

Mokbel, Mohamed F., Chi-Yin Chow, and Walid G. Aref. 2006. The new casper: Query processing for location services without compromising privacy. In *Proceedings of the 32nd international conference on very large data bases*, 763–774. VLDB '06. Seoul, Korea: VLDB Endowment.

Monreale, Anna, Dino Pedreschi, and Ruggero G. Pensa. 2010. Anonymity technologies for privacy-preserving data publishing and mining. In *Privacy-aware knowledge discovery: Novel applications and new techniques*, ed. F. Bonchi and E. Ferrari. Boca Raton: Chapman & Hall/ CRC Data Mining and Knowledge Discovery Series.

Narayanan, Arvind, and Vitaly Shmatikov. 2008. Robust de-anonymization of large sparse datasets. In *Proceedings of 29th IEEE symposium on security and privacy*, vol. 0, 111–125. Los Alamitos: IEEE Computer Society.

Ohm, Paul. 2009. Broken promises of privacy: Responding to the surprising failure of anonymization. *UCLA Law Review* 57:1701, 2010.

Opinion 4/2007 of the Article 29 data protection working party on the concept of personal data, WP 136, 20.06.2007.

Recommendation No. R (97) 5 of the Committee of Ministers to Member States on the protection of medical data, 13/02/1997.

Recommendation No. R (97) 18 of the Committee of Ministers to Member States on the protection of personal data collected and processed for statistical purposes, 30/09/1997.

Riboni, Daniele, Linda Pareschi, Claudio Bettini, and Sushil Jajodia. 2009. Preserving anonymity of recurrent location-based queries. In *Proceedings of the 16th international symposium on temporal representation and reasoning*, 62–69. TIME '09. Washington, DC: IEEE Computer Society.

Samarati, Pierangela, and Latanya Sweeney. 1998. Generalizing data to provide anonymity when disclosing information (abstract). In *Proceedings of the seventeenth ACM SIGACT-SIGMOD-SIGART symposium on principles of database systems*, PODS '98. New York: ACM.

Schwartz, Paul M., and Daniel J. Solove. 2011. The PII problem: Privacy and a new concept of personally identifiable information. *New York University Law Review* 86: 1814–1894.

Terrovitis, Manolis, and Nikos Mamoulis. 2008. Privacy preservation in the publication of trajectories. In *Proceedings of the ninth international conference on mobile data management*, 65–72. Washington, DC: IEEE Computer Society.

Winkler, William E. 1999. *The state of record linkage and current research problems*. Washington, DC: Statistical Research Division, U.S. Bureau of the Census.

Working Party document on data protection issues related to RFID technology, WP 105, 19/01/2005, Art. 8.

Xiao, Xiaokui, and Yufei Tao. 2006. Personalized privacy preservation. In *Proceedings of the 2006 ACM SIGMOD international conference on management of data*, 229–240. SIGMOD '06. New York: ACM.

Yakowitz, Jane. 2011. Tragedy of the data commons. *Harvard Journal of Law and Technology 25(1)*, Fall 2011.

Part II
Digital Natives and Ageing Users

Chapter 5
Digital Natives and the Metamorphosis of the European Information Society. The Emerging Behavioral Trends Regarding Privacy and Their Legal Implications

Norberto Nuno Gomes de Andrade and Shara Monteleone

5.1 Introduction

European Information society is going through a metamorphosis process as *digital natives* (hereafter, DN) are coming of age. This new generation of young people, who have grown up immersed in information and communication technologies (ICTs), reveal interesting attitudinal and behavioural patterns regarding the disclosure of personal information, profiling and protection of personal data.[1] How do these emerging attitudes, expectations and behaviours shape society and how does the current set of normative rules and principles enshrined in the existing European legal framework of data protection (DP) influence them? The objective of this article is to analyse how observed behavioural trends of digital natives regarding the protection of personal data should be taken into account in future revisions of the legal regulatory framework. For this purpose, the paper looks at the Better/Smart Regulation strategy of the European Commission (EC), proposing the incorporation of data collection on the behaviour and the attitudes of DN into the Impact Assessment (IA) procedures.

The research on digital natives is based on special Eurobarometer 359/2011 (EB), "Attitudes on Data Protection and Electronic Identity in the European Union"

[1] The authors acknowledge that, while the term 'digital natives' is widely used, its definitions vary: sometimes referring to teenagers, sometimes to adolescents and sometimes to all people under 35. For the purpose of this paper, we take into account the age categories used in the special Eurobarometer 359/2011 "Attitudes on Data Protection and Electronic Identity in the European Union", in which DN are identified in the young people aged 15–24. For a wide research study conducted in Europe on the Internet use among children and youngsters (aged 9–16) see the EU Kids Online project, www2.lse.ac.uk/media@lse/research/EUKidsOnline/Home.aspx.

N.N.G. de Andrade (✉) • S. Monteleone
IPTS, JRC, 3, Edificio EXPO C/Inca Garcilaso, Seville 41092, Spain
e-mail: Norberto.ANDRADE@ec.europa.eu; Shara.MONTELEONE@ec.europa.eu

S. Gutwirth et al. (eds.), *European Data Protection: Coming of Age*,
DOI 10.1007/978-94-007-5170-5_5,

(published by the European Commission in June 2011),[2] which constitutes the largest survey ever conducted on citizens' behaviours and attitudes concerning identity management, data protection and privacy.[3] We considered the main different behavioural patterns of DN, detected through this survey, focusing on their attitudes and perceptions in the disclosure of personal data via digital technologies. We based our claims also on a further analysis of the survey results developed by the EC-Joint Research Center-IPTS,[4] illustrating views, emerging attitudes and expectations of European citizens concerning their personal data. Moreover, we took into account the results of specialized studies and projects that looked upon the perceptions of privacy by DN, such as the PRACTIS project,[5] the EU Kids Online project[6] and other surveys conducted outside Europe.[7]

Based on the results of the literature mentioned above, we identified not only a generational gap between adults and younger people,[8] but also an important discrepancy between the legal dictates of the Data Protection Directive (according to which the processing of data is subject to rigorous legitimate criteria and principles) and the actual behaviour and privacy perceptions of the EU's youngest citizens. We also explore, among other topics, how one's experience of an invasion of privacy today may be different from the way it will be experienced in the future. Departing from such observations, we develop a series of underappreciated challenges between the legal and the social reality, the actual behaviour and privacy perception of the EU's youngest citizens. We advance the thesis that the current data protection legal framework may need to be stretched to adapt to future societal developments.

Taking into account the behaviours and attitudes of digital natives vis-à-vis the disclosure of personal data, we argue that European Data Protection law is running the risk of falling into a legally paternalistic temptation, rigidly protecting citizens

[2] This EB updates and integrates the Eurobarometer *Data Protection in the European Union: citizens' perceptions*, Analytical Report, February 2008, http://ec.europa.eu/public_opinion/flash/fl_225_sum_en.pdf.

[3] The survey was conducted in 27 EU Member States via a national, random-stratified sample of ~1,000 interviews; overall, 26,574 Europeans aged 15 and over were interviewed face-to-face in their homes, between 25/11 and 17/12 of 2010

[4] Wainer Lusoli, et al. *Pan-European Survey of practices, attitudes & policy preferences as regard personal identity data management*. JRC Scientific and Policy Reports, EUR 25295, available at http://is.jrc.eu.europa.eu/pages/TFS/eidsurvey.html

[5] http://www.practis.org/. Though the purpose of the PRACTIS project is to assess "the potential impacts of emerging and future technologies on privacy and privacy perceptions", and "how the developments of new technologies may induce shifts in perceptions about privacy", we deem that some of its main findings are valid to the aim of our paper, in particular those related to the possible generational gap between adults and younger people.

[6] http://www2.lse.ac.uk/media@lse/research/EUKidsOnline/Home.aspx.

[7] Chris Hoofnagle et al., *How different are Young adults from older adults when it comes to information privacy attitudes and policies* Survey, April 14, 2010, http://www.ftc.gov/os/comments/privacyroundtable/544506-00125.pdf.

[8] *Ibid*.

from the consequences of their actions and losing touch with the reality of data subjects' expectations and behaviours. As a consequence, we claim that future revisions of the legal framework should take into account the image of the emerging digital natives, recommending the introduction of specific DN behavioural data collection into IA procedures in the field of ICT lawmaking processes.

With this aim in mind, we developed our claims structuring the sections of this paper as follows. Section 5.2 defines digital natives, providing a review of the essential literature on the topic. Section 5.3 is devoted to discuss the emerging attitudes of younger people with regard the protection of their personal data and privacy as confirmed by data collected through recent studies. It reflects on new "perceptions" of privacy and considers, consequently, the legal implications of these emerging practices. Section 5.4 analyses the adequacy of the current DP legal framework in order to cope with new challenges and needs of the young generation. It elaborates specifically on three data protection paradigms that are increasingly being questioned by DN behavioural patterns: the principle of data minimization; the hierarchical mindset and the vertical architecture of the current DP model; and the requirement for systematic opt-in consent. Section 5.5 proposes a solution for the identified legal and social discrepancy by looking at the EU Better/Smart Regulation policy. In this ambit, we recommend the integration of collected data from DN into IA procedures, highlighting the importance of incorporating DN attitudinal and behavioural data in the EU lawmaking process. Finally, in section 5.6 we summarize our conclusions.

5.2 "Defining" Digital Natives

The concept of *digital natives* was first used in specialized literature on educational research by Marc Prensky, who contrasted the new generation of students, born and grown up in a world of information and communication technologies in the late 1980s and 1990s, to that of "digital immigrants" (hereafter, DI), who were born before the digital age and thus have had to adapt to new technologies.[9] As native speakers of the digital language of computers and the Internet, DN – according to Prensky – would think and process information in a fundamentally different manner.

The literature about DN is quite conspicuous, and initiatives that aim to 'understand' young people as they grow up in the digital age have proliferated around the word.[10] For this paper we reviewed selected studies that examine the nature, behavioral trends and technologies used by DN. These studies (which are not necessarily

[9] This definition is taken from Marc Prensky "Digital Natives, Digital Immigrants", in *On The Horizon. 6 MCB University Press* (2001).

[10] Further to Prensky's study, another focused research study on DN is the one developed by John Palfrey and Urs Grasser, *Born Digital*, New York: Basic Books, 2008. This work is the result of an ongoing interdisciplinary project of the University of Harvard and University of St Gallen, available at: http://www.borndigitalbook.com/.

focused on privacy issues, but often related to them) discuss whether DN, through their exposure to new technologies, have developed radically new cognitive capacities and learning skills besides being tech-savvy. The debates pivot on questions such as: do DN really think differently and learn differently? Is one born digital or does one become a DN? What is the role of technology in defining social movements?[11] It is interesting to note that a number of scholars debate and contest the idea that this generation is tech savvy.[12]

Though there is not a consensus on the nature and features of DN,[13] there is a general acknowledgement of quantitative differences in the use of technologies between DN and DI, as well as in their attitudes towards technologies.[14] These differences, moreover, may represent different needs, risks and opportunities for the new generation.

Aware of the existence of these current debates, our aim is not to add more knowledge to this literature base, nor to discuss the very nature of this discontinuity between generations. Instead, and taking into account these discussions, we intend to further stimulate the debate on the legal issues at play.

5.3 New Generations, New Technologies and New Privacy Perceptions

Since issues such as privacy online are not immediate concerns for most of the DN, at least when they are not directly asked about them,[15] one could simplistically infer from this statement that younger people are simply uninterested in these topics and

[11] See, *inter alia*, Nishant Shah and Fieke Jansen. *Digital AlterNatives With a Cause? Book One, To Be.* The Center for Internet and Society (CIS), 2011, http://www.scribd.com/nilofarh/d/65628308-Book-1-To-Be-Digital-Alternatives-With-a-Cause; See, moreover, David Buckingham. *Youth, Identity and Digital Media*, Cambridge: MIT Press, 2008; Rebecca Eynon and L. E. Malmberg (2011), A typology of young people's Internet use: Implications for education, 56 *Computers & Education* (2011): 585; Catrina Denvir, et al. "Surfing the web- Recreation or resource? Exploring how young people in the UK use the Internet as an advice portal for problems with a legal dimension", *Interacting with Computers* 23 (2011): 96-104; Yair Amichai-Hamburger, Gideon Vinitzky "Social network use and personality", 26 *Computers in Human Behavior*, 26 (2011) 1289.

[12] Sue Bennett et al. "The 'digital natives' debate: a critical review of the evidence" *British Journal of Educational Technology*, 39 (2008): 775. The difference between DN and older generation of users would lie in the appropriation of technologies, not in their ability to use it. Moreover, some scholars sustain that young people with Internet literacy tend to cope with more risks, but the level of exposure to online risks remains high also for those with lower Internet literacy: self-confidence, in fact, would go with more exposure to online risks. See also Sofie Vandoninck et al. "Digital Literacy among Flemish adolescents: How do they handle online content risks?" *Communications* 35 (2010): 397.

[13] For an overview on the different concepts regarding Digital Natives see: Michael Thomas, *Deconstructing Digital Natives, Young people and new literacy*, Routledge 2001.

[14] Anoush Margaryan et al. "Are digital natives a myth or reality?" *Computers & Education* 56 (2011) 429.

[15] See the study of Chris Hoofnagle et al., mentioned above.

that they do not care, as reported in most of the recent literature reflecting the digital natives discourse.[16] Nevertheless, one should be more cautions in drawing such conclusions and ask the following question: is it correct to simply say that DN do not care about the privacy risks they run when using new technologies?

From the results of the EB 359 survey, a number of meaningful figures emerge on the attitudes of European citizens regarding personal identity data, concerning, for instance the general use of Social Networking Sites (SNS) like *Facebook, Linkedin, Flickr, Youtube*, etc. According to the survey, more than a third of EU27 citizens (34 %) access SNS, and more than half of those (57 %) also use websites to share pictures, videos, music, etc. As the main use of SNS is to enable online socialising, it necessarily means disclosing social (personal) information online. One important conclusion is that SNS users (both DN and DI) seem less cautious than the non-SNS users about sharing information on the social networks, although they generally consider it personal.[17]

A relevant concept in relation to personal data disclosure is that of control, namely the amount of control SNS users think they have on data they disclose. One practical tool in relation to control is the ability to change one's privacy setting on a SNS profile from default. Overall, 56 % of SNS users surveyed affirmed that they have tried to change privacy settings of SNS personal profile from default options and 43 % have not tried. Hence, if SNS providers have not set appropriately high safeguards to protect people's personal data by default, this means that just less than half of European SNS users may have left their personal data unprotected in these environments.[18]

The survey also contains significant data concerning DN: In particular, it contains data on their behaviour regarding personal data and on the technologies they use in their daily activities, this information allows us to envisage future trends regarding personal data practices which should not be disregarded by policy makers. The survey, in fact, revealed a relevant generation split, as DN (the younger Europeans, still mostly studying, aged 15–24), are those who use the Internet more (94 %, EU 66 %), join SNS more (84 %, EU 52 %)[19] and use websites to share pictures, videos, movies more

[16] For an overview on the common discourse on DN in media, literature and education, built on the assumption that "youth do not care about privacy" see: Alice Marwick et al. "Youth, Privacy and Reputation", *Berkman Center Research Publication*, Harvard: Harvard University (2010).

[17] See EB 359, 45.

[18] Wainer Lusoli et al. "Pan-European Survey", 71. Interesting figures emerging from the EB 359 are also those related to control and responsibility perceptions of EU citizens using SNS. People thinking that disclosure is unavoidable are more likely to think they are responsible for protecting, rather than companies. People who are happy to disclose consider public authorities to be the ones responsible for the correct treatment of their data are responsible, rather than companies. However, there is no relation between self-responsibility and identity protection behaviours. Even people that feel responsible for their own data, do little to protect their personal data once they have been disclosed. This may be due to the lack of effective tools allowing people to take care of their data. But when tools are available, such as privacy notices, "responsible-feeling" people do read them. See Wainer Lusoli et al. "Pan-European Survey", 43.

[19] *Ibid.*, 39: "General pattern emerges from the socio-demographic analysis of the types of personal information disclosed on social networking or sharing sites. The younger the social or sharing site users are, the more likely they are to disclose their names (85 %), their photos (65 %), their nationality (54 %), the things they do (50 %), who their friends are (51 %) etc.".

(73 %, EU 44 %).[20] In all Member States DN tend to use the Internet very little outside SNS, while older people who use SNS are practically the same as the percentage of Internet users. DN perceive data disclosure as unavoidable (41 %, EU 28 %) and disclose more social information (48 %, EU 28 %). They also believe in strong uniform protection of their data and value their digital profile as much as older people. Furthermore DN also feel more in control and perceive less risk in using the Internet. The discrepancies that emerge between DN and DI strengthen our claim that policy and regulation of today will need to be overhauled in the short term.

Generational differences are confirmed also by the PRACTIS project's results that emphasize the contrast between the attention devoted by younger people to privacy concerns, when asked explicitly, and their behaviour.[21] From this contrast interesting considerations can be drawn:

Firstly, "adolescents perceive social network sites as part of their private sphere, where they exchange private information with their peers; secondly, they handle private data in a differentiated way trying to explicitly manage who gets which information. For the decision regarding which information is given to whom the context seems to matter. Finally, they are ready to trade off privacy for benefits, like discounts or increased convenience".[22]

Therefore, younger people do look for creating private spaces and do seek to control who gets what information according to which context. Meanwhile, when DN share information about themselves, increasing their exposure, they do so in order to obtain benefits of various sorts: "when they are negotiating privacy […] they are considering what they might gain from revealing themselves": this gain is not necessarily an economic gain (discount, free products or services), but could often be a reputational gain.[23]

Moreover, young people also reveal peculiar (and apparently contradictory) behavioural patterns. On the one hand, they appear more relaxed (in terms of personal data disclosure); on the other, they are more knowledgeable and alert. This aspect could seem paradoxical at a first glance, but it is not. This attitude can be understood as a product of the different perceptions and different needs of the new generation. Differences in privacy perception do not necessarily mean disregarding one's own personal data or ignoring the related risks connected with the data processing.

As DN are the citizens of tomorrow, it seems relevant to investigate what their perceptions of privacy is (and what it will be). It is likely that the existing generational

[20] See EB 359, 4.

[21] See PRACTIS Deliverable D3.4 final, Report on changing perceptions of privacy and the changing role of the State, http://www.practis.org/UserFiles/File/D3%204_final_report_20110725.pdf. One should note that the PRACTIS Report considers this behaviour as "privacy-treating behaviour", underlining younger peoples' lower awareness as regards privacy risks.

[22] *Ibid*, 7.

[23] danah boyd, Alice Marwick, Social Privacy in Network Publics: teens' Attitudes, Practices and Strategies, paper presented at Oxford Internet Institute's "A Decade in Internet Time: Symposium on the Dynamics of the Internet and Society" on September 22, 2011, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1925128, 10–13.

gap will expand and that, in the future, what is perceived today as a privacy concern will not be the same for the DN, who are already coming of age.

5.3.1 Is It True That Young People Do Not Care About Privacy?

Ralph Gross and Alessandro Acquisti,[24] scholars who have quantified individuals' willingness to provide large amounts of personal information in an online SNS and have inferred that the users are unconcerned about privacy risks, have nonetheless recognized the existence of different drivers influencing users' information revelation behaviour ("many simultaneous factors are likely to play a role"), acknowledging that the importance of which is still to be defined.[25]

According to the EB 359, DN feel sufficiently informed about the use of their data when joining a social networking, adapting their behaviour accordingly. They are likely to change their privacy settings and they are also likely to feel that they have control over the information disclosed on social networking In addition, they are more likely to appreciate the possibility of moving their data from one service provider to another.[26] As a general trend, today's young people use online spheres for peer socialization, relationship-building, information-sharing and mainly to talk with people they already know.[27] Young people, in the majority of cases, do want to put personal information online,[28] but this behaviour should not be automatically interpreted as a disregard for privacy. The data shown in the EB seems to suggest that this occurs not necessarily because they do not understand or do not care about risks,[29] but more likely because their perception of what is (and will be) private has changed. As Marwick stressed,

---

[24] Ralph Gross and Alessandro Acquisti, "Information Revelation and Privacy in Online Social Network (The Facebook case)", *Proceedings of the ACM Workshop on Privacy in the Electronic Society (WPES)*, New York, 2005.

[25] In subsequent research findings, the same authors (Alessandro Acquisti and Ralph Ross "Imagined Communities: Awareness, Information Sharing and Privacy on the Facebook", in *PET 2006*, ed. G. Danezis and P. Golle, Cambridge, LNCS 4258 (2006): 36) seemingly mitigated their assertions, acknowledging that members of communities do exhibit privacy concerns, though they are not deterred by them from joining the community.

[26] See EB 359, 160–167.

[27] Alice Marwick et al. 4.

[28] As Alice Marwick et al. highlight, the policy and technical solutions proposed until now are based on this assumption and presume that young people would not disclose their personal information if they understood the risks, consequently they focus predominantly on making DN aware of the consequences of disclosing information.

[29] James Grimmelman (2010), Privacy as Product Safety, 26 *Widener Law Journal*, 793, talks about these assumptions as "myths of privacy".

> much of the studies of privacy online focus on risk, rather than understanding the necessity of private spaces for young people where they can socialize away from the watching eyes of parents, teachers or marketers. These seeming contradictions demonstrate how understanding of risks, public space, information and the role of the Internet in day-to-day life differ between teenagers, parents […]and scholars.[30]

DN want private spheres. These are the spaces they have chosen for socialization, for free expression, for fun. These spaces are typically SNS or communities.[31] As Marwick et al. stress, young people, more than the adults, instead of viewing the public and private as two strictly separate realms, show a more flexible understanding of information disclosure and control. Consequently, "they want to be able to restrict personal data posted online in a *nuanced and granular way*" (emphasis added), "as posting personal information online is a way for youth to express themselves, connect with peers, increase popularity[…]".[32] They show an interest in controlling access to their personal information, by selecting – for instance – the set of information and the set of people to share this information with or finding particular practices to protect their privacy.

In boyd and Marwick' view, the idea that teenagers do not care about privacy is a widespread myth, "the participation in such networked publics does not imply that today's teens have rejected privacy as value".[33] These authors sustain that young people do have a sense of privacy, though their definitions of privacy vary widely. Accordingly, young people's practices in SNS would be shaped by their interpretation of the social situation and by their ability to navigate the *technological* and *social* environment, so that they would develop peculiar strategies to approach privacy aims. The technological architecture of SNS, which increasingly blurs the public/private dichotomy, would affect young people practices: "As social constructs, privacy and publicity are affected by what is structurally feasible and socially appropriate. In recent history, privacy was given as granted, because structural conditions made it easier to not share than to share. Social media have changed the equation".[34] Finally, these scholars offer a vision of privacy as a social norm

---

[30] Alice Marwick et al. 4. In a recent lawsuit in U.S., a Minnesota middle school student claimed a violation of her privacy rights by her school district, perpetrated through a search over her Facebook and emails account, confirming these different perceptions of privacy. See "Minnesota girl alleges school privacy invasion, March 10, 2012, http://articles.cnn.com/2012-03-10/us/us_minnesota-student-privacy_1_school-counselor-school-house-gate-facebook?_s=PM:US.

[31] Maria Karyda, Spyros Kokolakis Privacy Perceptions among Members of online Communities, in *Digital Privacy, Theories, Technologies and Practices*, ed. A. Acquisti, S. Gritzalis et al., New York: Auerbach Pub. (2008) distinguish different types of privacy: physical, interactional, psychological and informational privacy. Moreover they wonder how the concept of privacy protection may be affected by the fact that people online often have multiple (virtual) identities or profiles.

[32] Alice Marwick et al. 5.

[33] danah boyd, Alice Marwick, Social Privacy in Network Publics: teens' Attitudes, Practices and Strategies, paper presented at Oxford Internet Institute's "A Decade in Internet Time: Symposium on the Dynamics of the Internet and Society" on September 22, 2011, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1925128.

[34] *Ibid*., 10.

that is achieved through a wide array of social practices configured by structured conditions. In this light, young people seem to have started developing innovative strategies for achieving privacy: segmenting friends' groups depending on the service used (e.g., some teens use Facebook and Twitter to talk to different "communities"); or deleting constantly their comments or those of their friends after having read them; or even deactivating and reactivating on a daily base their Facebook account.[35]

As a consequence of the aforementioned young people's "nuanced and granular way" of using personal data on line and restricting the access to them, Heather West notices: "Rather than all-or-nothing public or private paradigm, we expect to be able to choose levels of privacy and levels of exposure to the public".[36]

Subsequently, policy and lawmakers should not further postpone taking into account young people's privacy practices. To say it with boyd and Marwick', "how teens approach privacy challenges the ways in which privacy is currently conceptualized, discussed, regulated".[37]

5.3.2 Changing Privacy Practices and Legal Implications

Despite being more inclined to disclose personal information, one can assert that DN will still become privacy-sensitive adults in the future. This is so because the contexts and the quality of their perceptions will be different as well as the practices and strategies used to protect their privacy.

This seems to be confirmed also by the findings of the PRACTIS study, which states that "adolescents' sensitivity for privacy seems to change towards a more flexible concept of privacy rather than diminish due to future technologies".[38]

A 2010 survey[39] on young American adults' attitudes (aged 18–24), reported by the Berkeley Center for Law & Technology, demonstrated that the picture is more

[35] danah boyd, Alice Marwick, Social Privacy in Network Publics, 18–20. See also Mimi Ito et al. Living and Learning with New Media: Summary of Findings from the Digital Youth Project. *The John D. and Catherine T. MacArthur Foundation Reports on Digital Media and Learning*, 52 (2008), http://www.itofisher.com/mito/weblog/2008/11/living_and_learning_with_new_m.html; and Emily Christofides, Amy Muise and Serge Desmarais, Information Disclosure and Control on Facebook: Are They Two Sides of the Same Coin or Two Different Processes? *CyberPsychology & Behavior*, 12(3), 341–345 2009.

[36] Heather West, Is Online Privacy a Generational Issue? *GeekDad, Wired.com*, 2009, http://www.wired.com/geekdad/2009/10/is-online-privacy-a-generational-issue/.

[37] *Ibid*.

[38] PRACTIS Deliverable D3.4 final, Report on changing perceptions of privacy and the changing role of the State, 7, http://www.practis.org/UserFiles/File/D3%204_final_report_20110725.pdf.

[39] Chris Hoofnagle et al., *How different are Young adults from older adults when it comes to information privacy attitudes and policies* Survey, April 14, 2010, http://www.ftc.gov/os/comments/privacyroundtable/544506-00125.pdf.

nuanced than portrayed in the popular discourse on DN (*e.g.*, they are less concerned about privacy). In that survey, Hoofnagle et al. note that the statements of American young adults reflected a sensitivity towards privacy and policy options, as well as a knowledge of information privacy law, which (only apparently) contrasted with their behaviour on SNS and elsewhere online.[40] The data of this survey, do not differ drastically from those emerging from the EB 359 or from the PRACTIS study. The latter, though, emphasizes the direct impact that new business models and new online practices (*e.g.*, selling personal data to third parties) exert on privacy threats and also on new privacy perceptions. We share, however, PRACTIS's view that the main threats to privacy induced by Internet companies are related to the lack of transparency towards users.[41] We also share the policy implications of these findings, namely the claim that Governments should regulate privacy by design for businesses, by – for instance – "imposing minimal standards on services and products, or implementing other process-oriented privacy assessment for technologies".

Our considerations on DN's changing perception of privacy are also in line with Nissenbaum's view of information privacy in terms of "contextual integrity" and its corollaries: (1) personal information is always tagged with the context in which it is revealed, that is, all sectors of life are governed by context-specific norms of information flow; (2) depending on the nature of information, in some contexts it is "appropriate" and expected to reveal and share certain information while in others it is not (Nissenbaum talks about norms of appropriateness that guide the behaviour of people in the different contexts); (3) daily people move into and out of different contexts (from family to business to leisure); the movement or transfer of information from one party to other(s) requires different levels of "distribution" of information, that correspond to different norms of information sharing.[42]

Still regarding the role of context, Gordon Hull et al.[43] sustain that "contextual gaps" are endemic to Facebook and other SNS, that these gaps are at the root of the many privacy issues, but also that these issues are mainly design issues, ameliorable by an interface design that could increase transparency and control of information flow. The development of new technologies, especially for SNS applications, tends to change the expected distribution norms of the perceived context (e.g. Facebook). Therefore, in order to allow the users to keep the control over the distribution of their information, SNS should render the flows of information on the site more transparent. In other words, as DN's perception of Facebook would be influenced by the design of the site, these gaps could be addressed through a "good" program design.

---

[40] Nonetheless, the Berkeley's report also presents data on the DN's lack of knowledge about the effective privacy protection ensured by the law. It concludes that the young adults do have an aspiration for increased privacy, but the business environment and other factors encourage them to disclose data in order to enjoy social inclusion. The suggestion from Hoofnagle et al. is, thus, to search for forms of assistance in the educational and regulatory field.

[41] PRACTIS Deliverable D3.4 final, 6.

[42] Helen Nissenbaum, "Privacy as contextual integrity", *Washington Law Review*, 79 (2004): 101.

[43] Gordon Hull, et al., Contextual Gaps: Privacy issues on Facebook, *Ethics and Information Technology*, 4, (2011): 289, http://ssrn.com/abstract=1427546.

Moreover, as pointed out by boyd and Marwick, teenagers do not share a uniform set of values about privacy and publicity. Variations in teens' practices seem, according to boyd and Marwick's view, to be "shaped by the social norms that surround them[…]Sharing is viewed differently in different friend groups, schools, communities".[44]

Following the insight of Marwick et al., on the need of DN – which not necessarily correspond to that of their parents – to restrict personal data posted online in a *nuanced and granular* way (i.e., using SNS in a multifaceted way, differentiating set of data/set of people according to the social contexts created online), we suggest that the focus of DN privacy discourse regarding SNS should consist in filling the existing "contextual gaps". We also suggest that an adequate legal framework should seek to assure a more context-based privacy protection, possibly with the support of technology, such as better program design for community sites.

Departing from the results of the survey and the analysis of the related literature and research conducted in this area, we shall argue in the following sections that there is not only a significant discrepancy between digital natives and non-digital natives, but also between the behaviors, practices and perceptions of DN regarding privacy and personal identity management and the data protection legal framework. In other words, we claim that there are a number of discrepancies between the legal dictates of the Data Protection Directive (DPD) and the actual behaviour and privacy perception of EU's young citizens, i.e. a growing mismatch between the social reality of DN and the legal reality of data protection. In effect, the existing legal framework does not seem to take into full account the emerging (and shifting) attitudes, expectations and behavioural trends of DN, reflecting instead a somewhat outdated vision of reality. Hence, the current regulatory scheme does not seem to be in pace with the reality of DN, i.e., with their new ways of communicating, sharing information, forming relationships, understanding privacy and perceiving their own identities.

Taking into account the behavior and attitudes of DN vis-à-vis the disclosure of personal data, we argue that European data protection law may soon fall into a legal paternalistic trap, shielding citizens from the result of their actions while drifting away from the reality of data subjects' expectations and behaviors.

It is in this context that we pose the question of whether and to what extent future legal revisions (namely the ones in the area of data protection) should take into account the new generation of users and their different attitudes and perceptions regarding the processing of their own personal data and the use of their electronic identities. In other words, the main question is to what extent the use of new technologies by DN and the behavioural trends that emerge from their utilization should be taken into account by the lawmakers in future legal revision processes.

[44] danah boyd, Alice Marwick, Social Privacy in Network Publics: teens' Attitudes, Practices and Strategies, paper presented at Oxford Internet Institute's "A Decade in Internet Time: Symposium on the Dynamics of the Internet and Society" on September 22, 2011, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1925128.

5.4 Current Legal Framework

The current international legal framework for privacy and data protection is based upon a set of instruments that date from the 1980s and 1990s, such as the 1980 OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (the "OECD Guidelines"), the Council of Europe Convention 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data ("Convention 108"),[45] and the European Union Data Protection Directive 95/46/EC ("DPD"). The DPD – the main European legal instrument on the protection of individuals with regard to the processing of personal data and on the free movement of such data – entered into force more than 17 years ago. At that time, technologies such as biometrics, social networking, cloud computing, web 2.0 or the Internet itself, were either non-existent or only making their first steps, still far from today's massive adoption and pervasive use. As Tene argues, the current legislative framework has not been able to keep up with these technological environment and remains based on concepts developed practically over 30 years ago.

> [T]he current Framework is in danger of being unraveled by a new generation of users utilizing a new generation of technologies. The fundamental concepts underlying the Current Framework, including basic terms such as 'personal data', 'data controller', 'data processor', and 'data transfer', have been disrupted by shifting technological realities.[46]

In this way, the current framework does not only refer to a completely different technological landscape from the one we have today, it still addresses the data subject of the 1990s and their lifestyles, privacy conceptions and needs. The new data subjects are, today, individuals who openly disclose and exchange large amounts of personal, often intimate, information online. DN are also, for example, the ones that transfer more information using peer-to-peer (P2P) file sharing applications.[47] They are individuals used to having their location tracked, their profiles displayed, their photos posted, and their tastes and preferences revealed. Their daily lives are increasingly entrenched and dependent upon the information they constantly produce, seek and receive in the online and offline spheres.

---

[45] The OECD Guidelines and the Convention 108 were, in effect, put in place before the advent of the World Wide Web as a public network.

[46] Omer Tene, Privacy: The New Generations. *International Data Privacy Law* 1 (2011).

[47] In a recent empirical study that characterizes and quantifies the amount of content of various types that is transferred worldwide using BitTorrent, it was found that content that is popular among teenagers is more likely to be disproportionately represented in BitTorrent as compared to content that appeals to an older audience. See, MATEUS, A. M. & PEHA, J. M. 2011. Quantifying Global Transfers of Copyrighted Content Using BitTorrent *39th Telecommunications Policy Research Conference (TPRC) 2011* George Mason University School of Law, Arlington, VA.. This study has also concluded that BitTorrent Transfers result in hundreds of millions of copyright violations worldwide per day, and that copyright holders fail to realize significant revenues as a result. The analysis of this result in light of DN behavior practices lead us to discuss the adequacy and the (social) acceptance of current copyright laws (and the need to devise new alternative models to the existing one). The analysis of DN behavioural trends may also prove to be useful in the revision of copyright laws. Nevertheless, this discussion goes beyond the scope of this paper.

Contrarily to what the existing data protection rules seem to imply, there are important benefits to withdraw from maximizing the disclosure and sharing of information. As Swire contends, and "[a]s illustrated by our eagerness to use social networks, access to the personal data of others is often a benefit to individuals, rather than the threat assumed by the data protection approach. These benefits notably include our right to associate, to reach out to people to effect political change and realize ourselves as individuals".[48]

Nevertheless, the current DPD still presents the same structure, the same set of basic principles and rules, and the same mindset of 1995 – when the "Internet" was still in an embryonic phase. The current data protection legal framework is based upon a set of unquestioned premises and paradigms that are, notwithstanding, being slowly disrupted by shifting technological developments and user's practices and perceptions.[49] In the following we take a closer look at three of these paradigms.

5.4.1 Minimization of Information

The effective protection of personal data relies upon the robust application of principles such as purpose limitation and the minimization of personal data collection, as required by the EU Data Protection Directive. One of the key principles of the current data protection legal framework is thus the principle of data minimization.

This principle derives from Article 6.1 (b) and (c) of DPD, which states that personal data must be "collected for specified, explicit and legitimate purposes" and must be "adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed". According to this principle, a data controller should limit the collection of personal information to what is directly relevant and necessary to accomplish a specified purpose. Moreover, data controllers should also retain the data only for as so long as is necessary to fulfill that purpose. Briefly, the data minimization principle requires data controllers to collect only the personal data they really need and to keep it only for as long as they need it.[50]

---

[48] SWIRE, P. 2012 Social Networks, Privacy, and Freedom of Association: Data Empowerment vs. Data Protection *North Carolina Law Review, 2012; Ohio State Public Law Working Paper 165; 2011 TPRC Conference.*

[49] The inefficiencies and shortcomings of the current data protection model, such as the ones developed in this section, have led legal scholars and computer scientists to put forward alternative models, presenting different proposals of how to attain a more effective enforcement of one's privacy and data protection rights. This is the case of the proposal for introducing property rights in personal data (see Purtova, Nadezhda. *Property Rights in Personal Data. A European Perspective*, Kluwer Law International 2012.) or the proposal of a data protection approach based on the assertion of different categories of privacy harms (see CALO, M. R. 2011). The Boundaries of Privacy Harm. *Indiana Law Journal,* 86.

[50] http://www.edps.europa.eu/EDPSWEB/edps/site/mySite/pid/74.

While the legal "rhetoric" of the current framework emphasizes the construction of an information ecosystem where individuals and organizations interact with one another on the supposed basis of minimized disclosure of personal information, the technological reality is completely different, not to say the exact opposite. In fact, we are living and participating in "an online reality that is optimized to increase the revelation of personal data".[51] Steady increases in processing power allow more information to be extracted about individuals, employing data mining algorithms to discern and record patterns of behaviour,[52] and generating more and more information. In addition, and along the lines of the pervading Web 2.0 business model, users are encouraged to maximize their personal data by producing digital content, sharing information, forming relationships and establishing networks,[53] which are then used and exploited by commercial companies and other entities. The internal logic of Web 2.0 is thus structured, on the one hand, on users who are converted into *superprocessors* of information and, on the other hand, on business companies that seek to surveil every user action, store the resulting data and mine it for profit.[54]

Rather than data minimization, one should emphasize the value and of benefits of data maximization (the increased production and access to personal data), as well as the need for data empowerment.[55] Contrarily to data protection, which relies on limits to sharing of information, data empowerment relies precisely on information sharing, allowing ordinary people (through the use, for instance, of social media tools) to do things with personal data that only large organizations used to be able to do.[56]

---

[51] Chris Hoofnagle et al. "How Different are Young Adults from Older Adults", 20.

[52] Ian Brown, Data Protection: The New Technical and Political Environment. *Computers & Law* 20 (2010).

[53] This mode of computing has been called "affective processing", see Robert, W. Gehl, The Archive And The Processor: The Internal Logic Of Web 2.0 *New Media & Society* 13 (2011): 1228.

[54] *Ibid*. Surveys on privacy attitudes seem to suggest that some of today's SNS users are aware of (and comfortable with) this commercial environment, while others are not. It needs further monitoring to see to what extent these attitudes might change over time.

[55] *Ibid*.

[56] Peter Swire. 2012 Social Networks, Privacy, and Freedom of Association: Data Empowerment vs. Data Protection *North Carolina Law Review, 2012; Ohio State Public Law Working Paper 165; 2011 TPRC Conference.* "I suggest the term 'data empowerment' to describe how individuals use personal data in social networks and the other many horizontal relationships enabled by modern computing … the 2008 Obama campaign and the Arab Spring symbolize the political dimension of this empowerment. The discussion of non-profit, religious and other expressive associations shows that the empowerment goes well beyond the realm of political power. More broadly, individuals are empowered to reach out to others on many dimensions, from the cultural (writing, photos, music), to the economic … to the everyday social interactions of the social networks themselves", Peter Swire. 2012 Social Networks, Privacy, and Freedom of Association: Data Empowerment vs. Data Protection *North Carolina Law Review, 2012; Ohio State Public Law Working Paper 165; 2011 TPRC Conference.*

The current technological environment, where business models encourage users to disclose personal information and where the users (namely the DN) happily do so, not only questions the adequacy of the current legislative framework, but also its effectiveness.[57] Taking into account the avalanche of data that is being produced and the multifarious purposes to which they are used for, what is the actual use and effectiveness of the data minimization principle? Is it still possible to uphold it? Or better, does it still make sense? In this light, it is important to note that the sole focus on data minimization obfuscates the benefits of data sharing for consumers. Notwithstanding the control one should have over his or her data, the fact is that the maximization of this data may also bring relevant advantages to the user. In effect, behavioral ads are overwhelmingly appreciated by consumers.

In brief, the minimization of the processing of information required by the existent legal framework is becoming somewhat unrealistic, unattainable and, moreover, at odds with the current and forthcoming technological environment, business models and user practices regarding privacy, identity and data protection.

5.4.2 Hierarchical Mindset/Vertical Architecture

The DPD is aimed at protecting the privacy of individuals by bringing within its scope the information processing activities of companies and organizations that collect and extract information from these individuals. The European Data Protection Directive is thus structured in a hierarchical fashion according to which the information stream is depicted vertically,[58] flowing from the data subjects – usually perceived as individual physical persons – to the data controllers and processors – larger companies and institutions. In principle, the DPD does not cover horizontal relations, i.e., information flows among individual persons. The Directive, in effect, establishes in its Article 3/2 the so-called "household exemption", according to which its rules do not apply to individuals who process personal data for "purely personal purposes"

[57] Furthermore, in a recent empirical study regarding how privacy laws affect the location decisions of Internet firms when faced with high legal standards of privacy protection, the ease of access to personal data proved to be a determinant factor. In effect, the study demonstrated that the more a jurisdiction makes collecting and using these data easy, the more attractive the country is. Such analysis highlighted a new privacy paradox according to which the more stringent certain online privacy laws are, the more they induce firms to locate their business in less stringent countries, and finally the weaker actual privacy protection on the internet is. See, Fabrice Rochelandet & Silvio H.T. Tai 2012. Do Privacy Laws Affect the Location Decisions of Internet Firms? Evidence for Privacy Havens Available: http://ssrn.com/abstract=2022160.

[58] See also, in this respect, Peter Swire. 2012 Social Networks, Privacy, and Freedom of Association: Data Empowerment vs. Data Protection. The author also depicts the shift from vertical to horizontal relationships in computing.

or "in the course of a household activity". In other words, data protection principles and rules do not apply to individuals who make use of personal data just for their own domestic and recreational purposes.

Taking into consideration the ever-increasing merge between public and private spheres and caused by the various developments observed in the field of ICT, the understanding that the DPD had of "purely personal" back in 1995 is today open to discussion and interpretation. In inserting, in the mid-1990s, the so-called "household exemption", the DPD assumed that personal data processed for domestic purposes did not raise privacy risks or issues of responsibility on the side of the data controller, as he or she would only be processing the data for their own private purposes. The directive also departed from the assumption that the processing of data for personal purposes (horizontal relations) would only involve a restricted circle of intimate people and, as such, would not entail the expectation or the need to protect the privacy of the individuals identified. With the rise and consolidation of social networking sites (SNS), these assumptions are highly questionable today. In fact these assumptions are at odds with today's reality and, moreover, with the behavioral trends of DN. The publishing of personal information on SNS, even if for purely personal or recreational reasons, often involves the disclosure of information to large audiences.[59] And this contradicts the assumption that data will only circulate among a restricted circle of people and that its disclosure does not represent any privacy risk.[60] The sharing of information among SNS users also puts into question the definition of "data controller" within the Data Protection Directive. If this definition – a "natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data" – is applied literally to SNS then not only organisations such as Facebook or Google Plus would be regarded as "data controllers" (through Art. 4 of the DPD), but also individuals who posted information about others would also be regarded as "data controllers" and thus would have to adhere to the DPD rules.[61]

[59] The average Facebook user has 130 friends and is connected to 80 community pages, groups and events (http://www.facebook.com/press/info.php?statistics).

[60] Art. 29 WP has clarified a number of instances where the activity of an SNS may not be covered by the household exemption, namely "when the SNS is used as collaboration platform for an association or company" or "when access to profile information extends beyond self-selected contacts, such as when access to a profile is provided to all members within the SNS or the data is indexable by search engines." As noted in its Opinion, "a high number of contacts could be an indication that the household exception does not apply and therefore that the user would be considered a data controller", Article 29 Working Party, Opinion 5/2009 on online social networking, 2009b, http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp163_en.pdf.

[61] Rebecca Wong, "Social networking: a conceptual analysis of a data controller". *Communications Law* 14 (2009): 142–149.

There is thus an urgent need to review the adequacy of the hierarchical model and vertical focus of the current data protection legal framework (data controller – data subject),[62] as well as to clarify the rules applying to data processing by individuals for private purposes, that is, at a horizontal level.[63]

5.4.3 Consent

In the context of Data Protection legislation, consent is one of the requirements for the lawful processing of personal data. It corresponds to any freely, given, specific and informal indication of the wishes of a data subject, by which he or she agrees to the processing of personal data related to them.[64] The obtained consent, moreover, can only be used for the specific processing operation for which it was collected.

Despite the importance of consent to the protection of a data subject's privacy, it is important to bear in mind that an excessive dependence on consent may overload the user's online experience. Moreover, the constant requirement of opt-in consent for the collection and processing of data is not in line with DN's browsing and navigating habits.[65]

---

[62] Despite recognizing the lack of safeguards that need to be addressed for individuals who upload their own personal data into the internet (social networks, cloud computing services, etc.), Art. 29 WP "does not recommend, however, revising the terminology used in the Data protection framework for data controller and data subject relationship in the context of Web 2.0 technologies or cloud computing, but rather, to continue using the 'data controller – data subject' dichotomy and enhancing their responsibilities, which appears by some outmoded in Web 2.0 technologies" – Rebecca Wong, "Data protection: The future of privacy". *Computer Law & security Review* 27(2011): 53. See also Article 29 Working Party 2009a. The Future of Privacy. Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data.

[63] In this light, a number of questions may be posed: What is to be understood by "purely personal purposes"? Does the posting of information on an SNS equate to the disclosure of information for private purposes, that is, to our private (although admittedly large) group of selected contacts? Or – depending on the access to the information – does it equate to disclosure of information to the public? How many people with access to that information would render its diffusion as processing of personal data for private purposes or, instead, as disclosure to the public?

[64] See Article 2 (h) of DPD and article 2 (h) of Regulation (EC) No 45/2001.

[65] The systematic need for opt-in consent is also out of touch with the ubiquity of current and future mechanisms of data processing, rendering ineffective the existing notice and choice regime. In effect, with the forthcoming development of the Internet into an Ubiquitous Computing environment (also called Ambient Intelligence or Internet of Things), the current opt-in consent model is frankly not sustainable in the long run. The trend is to move towards a frictionless, mobile and ubiquitous technological environment in which the request for permanent consent will be extremely difficult to articulate. For an overview of the technological developments leading towards an Ambient Intelligence Scenario, see Norberto Andrade, Technology and Metaphors: from Cyberspace to Ambient Intelligence. *Observatorio (OBS*) Journal* 4 (2010): 121–146. For an overview of the challenges posed by the vision of Ambient Intelligence, see Antoinette Rouvroy, Privacy, Data Protection, and The Unprecedented Challenges of Ambient Inteligence *Studies In Ethics, Law, And Technology,* Berkeley Electronic Press (2008).

Proposals to solve the problem of the burdensome requirement for constant consent include software agents, deemed as an effective way to achieve the protection of privacy, particularly challenged by new Information Technologies. The underlying idea is that a technological architecture based on 'Privacy Agents', which meets a series of legal requirements to ensure the validity of consent delivered through such agent, could be useful to avoid overwhelming the data subject with repeated requests of consent, while protecting his/her privacy. This option,[66] thought for the general Internet users, would certainly be very welcomed by to DN users.

5.5 Digital Natives and the EU Lawmaking Process

In order to increase the effectiveness and reduce the overall costs of regulation, the EU has been for more than a decade engaged in improving the quality of its lawmaking processes, instruments and outcomes. These efforts can be grouped into what has been called "Better Regulation" (BR) policy, recently re-labeled as "Smart Regulation" strategy. Taking into account that, among its various objectives, BR "seeks to ensure that decision-making meets the needs and expectations of citizens",[67] we argue that a tighter connection should be established between DN (namely their expectations) and the EU lawmaking process. The latter should, moreover, strive to understand the behavioral trends of these young citizens, adapting its rules in a way that fosters the desirable behaviors and prevents the non-desirable ones. In this section, we propose and explain how EU lawmaking process could (and should) take into account collected data from DN (behavioral, cognitive, etc.), namely in the ambit of the so-called impact assessment (IA) procedures.

5.5.1 Better/Smart Regulation

As more and more laws applicable in the EU Member States (MS) have their origin in EU-decision-making processes, the need to simplify and improve the quality and effectiveness of the regulatory environment has progressively assumed greater importance on the EU agenda. In order to achieve these goals, the European Commission (EC) has deployed a detailed strategy and policy of "Better

[66] Daniel Le Metayer and Shara Monteleone, "Automated Consent through Privacy Agent: legal requirements and technical architecture", *Computer Law Security Review* 25 (2009) 136–144.

[67] Lorenzo Allio, L. 2007. Better regulation and impact assessment in the European Commission. *In:* Colin Kirkpatrick & David Parker (eds.) *Regulatory Impact Assessment. Towards Better Regulation?* Cheltenham, UK: Edward Elgar.

Regulation",[68] devising a series of different processes, structures and tools to prepare new legislation (looking at new initiatives proposals still under negotiation) and to review the existing one (legislation already enacted).[69] In this light, the Better Regulation program includes a mix of different actions:

– "introducing a system for assessing the impact and improving the design of major Commission proposals;
– implementing a programme of simplification of existing legislation; testing Commission proposals still being looked at by the Council of Ministers and the European Parliament, to see whether they should be withdrawn;
– factoring consultation into all Commission initiatives;
– looking at alternatives to laws and regulations (such as self-regulation, or co-regulation by the legislator and interested parties)."[70]

In its overall goal to prepare and apply the best regulatory tools at the EU level, the BR strategy is articulated in three key actions: simplification, reduction of administrative burdens and impact assessment. In the following, we look at the latter.

5.5.2 Impact Assessment (IA)

A crucial element in producing better laws is to anticipate and acknowledge their likely impacts. In this way, the Commission "has focussed on IA as the key element for its BR agenda",[71] rendering it compulsory for major policy proposals.

The IA[72] is a "tool that assists regulators in their efforts to structure decision-making and increase the effectiveness of regulatory outcomes".[73] It is a threefold

[68] See ec.europa.eu/governance/better_regulation/index_en.htm. The Better Regulation policy had its origin in 2001 with the Mandelkern report on Better Regulation. For an evolution of the "better/smart regulation" agenda at the level of the EU, see *Ibid*. Helen McColm. 2011. Smart Regulation: The European Commission's Updated Strategy. *European Journal of Risk Regulation***,** 9–11. Lorenzo Allio. 2011. On the Smartness of Smart Regulation – A Brief Comment on the Future Reform Agenda. *European Journal of Risk Regulation*.

[69] Furthermore, by re-labeling the strategy "Smart Regulation", the EC has connected the two extremes of the policy cicle, enhancing the ex ante impact assessment of a given proposal, while devoting more attention to the ex post evaluation and outcomes of the produced legal instrument. See Helen Mccolm. 2011. Smart Regulation: The European Commission's Updated Strategy. *European Journal of Risk Regulation***,** 9–11.

[70] European Commission 2006. Better Regulation – Simply Explained. Luxembourg: Office for Official Publications of the European Communities.

[71] Lorenzo Allio. 2007. Better regulation and impact assessment in the European Commission. *In:* Colin Kirkpatrick & David Parker. (eds.) *Regulatory Impact Assessment. Towards Better Regulation?* Cheltenham, UK: Edward Elgar.

[72] See, in general, Anne Meuwese, 2008. *Impact Assessment in EU Lawmaking,* The Hague, Kluwer Law International.

[73] Lorenzo Allio. 2010. Keeping the Centre of Gravity Work: Impact assessment, Scientific Advice and Regulatory Reform. *European Journal of Risk Regulation***,** 76–81.

system that assesses and analyses the economic, social and environmental impacts of a proposal. The IA is linked to the preparatory stage of policy-setting and decision-making on the one hand, and the revision of the *acquis communautaire*, on the other.[74] In effect, IA is progressively being understood as a "wide-ranging 'process'[75] structuring and closing the policy-making cycle, influencing and supporting the various different aspects of the Better Regulation policy".[76] Moreover, the IA consists of "a knowledge-based approach – aimed at ensuring that decisions on whether and how to proceed with an initiative are based on solid evidence and a thorough analysis of options".[77]

In more detail, IA is a set of logical steps to be followed when preparing policy proposals; it is a process that prepares evidence for political decision-makers on the advantages and disadvantages of possible policy options by assessing their potential impacts (the results of this process are then summarised and presented in the IA report).[78] At a more technical level, the carrying out of an IA is composed by the following key analytical steps: identifying the problem, defining the objectives, developing main policy options, analysing the impacts of the options, comparing the options, and outlining policy monitoring and evaluation.[79]

5.5.3 Integrating Digital Natives into the IA system

In the ambit of Smart Regulation consultation exercises, and regarding the effort to improve the transparency of the process, the Commission strives to hear the views of all interested parties, namely those of SME (small and medium-sized enterprises), non-governmental organizations representing vulnerable stakeholders and citizens. Nevertheless, and further to allowing (and incentivizing) stakeholders to comment on planned impact assessments (by publishing 'roadmaps' outlining its plans for the broad direction of proposals, the public consultation process and supporting analysis),

---

[74] Lorenzo Allio. 2007. Better regulation and impact assessment in the European Commission. *In:* Colin Kirkpatrick & David Parker. (eds.) *Regulatory Impact Assessment. Towards Better Regulation?* Cheltenham, UK: Edward Elgar.

[75] As a process, IA "naturally spills over into the development of other equally crucial elements of regulatory reform, such as enhanced planning and programming; systematic and timely consultation practices, a smoother implementation and enforcement of legislation, and enhanced transparency and accountability" Lorenzo Allio. 2010. Keeping the Centre of Gravity Work: Impact assessment, Scientific Advice and Regulatory Reform. *European Journal of Risk Regulation*, 76–81.

[76] *Ibid*.

[77] European Commission 2006. Better Regulation – Simply Explained. Luxembourg: Office for Official Publications of the European Communities.

[78] European Commission 2009. Impact Assessment Guidelines.

[79] For a detailed description of these key analytical steps, along with practical examples of how they have been carried out in previous IAs, see *Ibid*.

the EC should also integrate DN (as an important and specific category of stakeholders) in the very process of impact assessment regarding legislative proposals in the field information and communication technologies (ICT) regulation. In other words, the process of gathering valuable input from stakeholders should not be restricted only to consultation exercises (which are obviously welcome), but involve also the gathering of empirical collective data from specific legal addressees, such as the DN.

In this respect, and further to IA's focus on reducing the administrative burden and compliance costs imposed on economic operators by regulation, we argue that IAs should also address the likely impacts of (ICT) regulation by identifying and understanding the behavioural trends of the users of new technologies and the addresses of the legal instruments under scrutiny, The evidence gathered through the examination of DN behavioural trends may prove to be extremely useful in the development of possible policy options in the IA exercise, along with the analysis of the options' impacts.

Moreover, the collection of data regarding the behavioural, cognitive and attitudinal trends of DN (and the assessment of how the latter impact on current legislation) is in line with the efforts that the Commission has put on reforming the way scientific advice is collected, validated and used throughout the decision-making process. This is particularly evident in the 2009 revised IA Guidelines, which "reinforce the requirement for desk-officers to rely on data that is of high quality".[80] The collection and use of DN reliable data requires the further integration of this particular category of stakeholders into the IA exercise in particular, and in the EU lawmaking structure in general. Along this process, DN move from mere and passive addressees of laws to active contributors and shapers of the latter.

As a way to complement and support the diffusion of comprehensive IA processes, and as a reinforcement of the principle of evidence-based decision-making, we thus propose the incorporation of specific DN data collection and analysis into the impact assessment procedures of ICT legal proposals. This recommendation could also contribute to solving the tendency for law and regulation, namely with regard to computer and communications sector, to become increasingly detailed and overly complex.

Despite the alleged benefit of increasing their certainty as to compliance, and as noted by Reed, over-complex laws have their normative effort greatly weakened, becoming also contradictive and subject to frequent amendment processes.[81] As a solution, Reed proposes to abandon the search for certainty and to adopt a method of lawmaking which seeks to influence behaviour by requiring the law's subjects to make their own qualitative assessments as to whether they were meeting the obligations imposed on them.[82] This proposal could be used in the specific case of DN,

[80] Lorenzo Allio, 2010. Keeping the Centre of Gravity Work: Impact assessment, Scientific Advice and Regulatory Reform. *European Journal of Risk Regulation*, 76–81.

[81] Chris Reed, 2010. How to Make Bad Law: Lessons from the Computing and Communications Sector *Queen Mary School of Law Legal Studies Research Paper No. 40/2010*.

[82] *Ibid*.

inviting the legislator to approach directly this specific category of legal subjects, assert if they were complying with the obligations established in law, and – in the case of a negative response – understand why they were not. Engaging into qualitative assessments of law's subjects "will not only make the law more easily understandable by those to whom it applies, but will also increase the normative effect of computer and communications law".[83] Reed's proposed lawmaking approach, which concentrates on human actors rather than on the technological activities those actors engage in,[84] is in line with our own proposal of integrating DN collected data to the impact assessment procedures of ICT laws or legislative proposals. Using the scholar's methodology, and replacing the terms laws with the one of IA, the latter should thus:

– "Identify the behaviours which are likely to emerge from the innovation they want to regulate;
– Decide which behaviours are to be fostered and which discouraged; and
– Devise mechanisms for persuading the human actors to behave in the desired manner"[85]

In this way, IAs would reinforce the regulators' capacity to meet the societal expectations of legal subjects. Moreover, IAs would also prepare laws designed according to the legal addressees' current and prospective behavioural, attitudinal and cognitive trends, reinforcing the overall effectiveness of the regulatory environment.

This remodeled IA proposal would allow lawmakers to better understand DN attitudes regarding personal data and identity protection and to shape future laws according to their corresponding needs and expectations. In specific, the legislator would be able to identify areas where a stricter regulation would be necessary (such as in the field of profiling and its unintended consequences); and identify other areas where a less stringent approach would be more opportune (such as in the field of the systematic opt-in consent).

5.6 Conclusion

The Art. 29 Working Party has confirmed that, despite the emergence of new technologies and the galloping pace of the globalization trend, the main principles of data protection are still valid and applicable. According to the WP, "the level of data protection in the EU can benefit from a better application of the existing data protec-

[83] *Ibid*.

[84] *Ibid*.

[85] *Ibid*. As a concrete example of an existing law redrafted to fit such lawmaking approach, Reed proceeds to a partial redraft of data protection law which aims to comply with the principles of law-system quality. See, Chris Reed. 2010. How to Make Bad Law: Lessons from the Computing and Communications Sector.

tion principles in practice".[86] This assertion is, nevertheless, limited. It looks at the objective factors of technology development and not to the subjective factors of perception, habit, preference and understanding of the users of these new technologies.[87] Hence, future revisions of the data protection legal framework should not only be promoted taking into account new technological developments, but also – and mainly – the new data subjects[88] and their behavior.

We thus argue that future revisions of DPD legal framework (namely their corresponding IA exercises) should also take into account the image of the emerging DN, recommending a higher degree of flexibility in the application of its rules. This will allow legal systems to become closer to the legal subjects and to be more effective in the application of its rules.

The approach to EU lawmaking processes advocated in this article is an inherently prospective one. In this respect, law should bear in mind that DN will in a couple of years, become adults and that they should, as such, not only be shaped by what Law says but also influence how Law should be. Law-makers should thus learn to look at the future, to foresee and to anticipate the needs and the changing perceptions of those who are DN of today and adult citizens of tomorrow. In effect, the current framework should strive not only to adapt itself but also to anticipate both forthcoming technological landscape and their future users.

In his attempt to devise an empirical measurement of law-system quality, Schmidt observes that the "quality of a law system is not only related to its success in fulfilling the requirements of the design (…), it is also related to its capacity to attract people, (…) to generate willingness to participate."[89] Nevertheless, the reality of data protection regulation is progressively striding away from the reality of its addressees, namely from the digital natives and their current perceptions and practices of privacy. This article aims to call the attention to this fact and to the need to bridge the legal reality with the social one.

References

Alessandro Acquisti and Ralph Ross. 2006. Imagined communities: awareness, information sharing and privacy on the facebook. Proceedings of Privacy Enhancing Technologies Workshop (PET) 2006, LNCS 4258, Springer: 36–58.

Allio, Lorenzo. 2007. Better regulation and impact assessment in the European Commission. In *Regulatory impact assessment. Towards better regulation?* ed. C. Kirkpatrick and D. Parker. Cheltenham: Edward Elgar.

[86] Article 29 Working Party, "The Future of Privacy. Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data", 2009a. http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp168_en.pdf.

[87] It is obvious that perception – as a subjective factor – is inexorably influenced and shaped by the technological environment – objective factor – surrounding them.

[88] "Not only technology has changed over the past 30 years: the individuals using it have changed too", Omer Tene, "Pivacy: The New Generations", *International Data Privacy Law* 1 (2011).

[89] Aernout Schmidt. 2009. Radbruch in Cyberspace: About Law-System Quality and ICT Innovation. *Masaryk University Journal of Law and Technology,* 3.

Allio, Lorenzo. 2010. Keeping the centre of gravity work: Impact assessment, scientific advice and regulatory reform. *European Journal of Risk Regulation*.
Allio, Lorenzo. 2011. On the smartness of smart regulation – A brief comment on the future reform agenda. *European Journal of Risk Regulation* 1: 19–20.
Amichai-Hamburger, Yair, and Gideon Vinitzky. 2011. Social network use and personality. *Computers in Human Behavior* 26: 1289–1295.
Andrade, Norberto. 2010. Technology and metaphors: From cyberspace to ambient intelligence. *Observatorio (OBS*) Journal* 4: 121–146.
Article 29 Working Party. 2009a. The future of privacy. Joint contribution to the consultation of the European Commission on the legal framework for the fundamental right to protection of personal data. http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp168_en.pdf.
Article 29 Working Party. 2009b. Opinion 5/2009 on online social networking. http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp163_en.pdf.
Bennett, Sue, Karl Maton, and Lisa Kervin. 2008. The 'digital natives' debate: A critical review of the evidence. *British Journal of Educational Technology* 39: 775–786.
Boyd, Danah and Alice Marwick. 2011. Social privacy in network publics: Teens' attitudes, practices and strategies.. Paper presented at Oxford Internet Institute's "A Decade in Internet Time: Symposium on the Dynamics of the Internet and Society". http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1925128. Accessed 22 Sept 2011.
Brown, Ian. 2010. Data protection: The new technical and political environment. *Computers and Law* 20(6): 40–42.
Buckingham, David. 2008. *Youth, identity and digital media*. Cambridge, MA: MIT Press.
Calo, Ryan. 2011. The boundaries of privacy harm. *Indiana Law Journal* 86: 1131.
Center for Democracy and Technology Policy Post. 2009. The dawn of the location-enabled. https://www.cdt.org/policy/dawn-location-enabled-web.
Denvir, Catrina, Nijel J. Balmer, and Pascoe Pleasence. 2011. Surfing the web – Recreation or resource? Exploring how young people in the UK use the internet as an advice portal for problems with a legal dimension. *Interacting with Computers* 23: 96–104.
European Commission. 2006. *Better regulation – simply explained*. Luxembourg: Office for Official Publications of the European Communities.
European Commission. 2009. *Impact Assessment Guidelines*. Luxembourg: Office for Official Publications of the European Communities.
Eynon, Rebecca, and L.E. Malmberg. 2011. A typology of young people's internet use: Implications for education. *Computers in Education* 56(3): 585–595.
Gehl, Robert W. 2011. The archive and the processor: The internal logic of web 2.0. *New Media and Society* 13(8): 1228–1244.
Gordon, Hull, Heather R. Lipford, and Celine Latulipe. 2011. Contextual gaps: Privacy issues on Facebook. *Ethics and Information Technology* 13(4): 289–302. http://ssrn.com/abstract=1427546.
Grimmelman James. 2010. Privacy as product safety. *Widener Law Journal* 19: 793.
Gross, Ralph and Alessandro Acquisti. 2005. Information revelation and privacy in online social network (The Facebook case). In *Proceedings of the ACM workshop on privacy in the electronic society (WPES)*, New York: ACM.
Hoofnagle, Chris, Jennifer King, Su Li, and Joseph Turow. 2010. How different are young adults from older adults when it comes to information privacy attitudes and policies?. Survey. http://www.ftc.gov/os/comments/privacyroundtable/544506-00125.pdf. Accessed 14 Apr 2010.
Karyda, Maria, and Spyros Kokolakis. 2008. Privacy perceptions among members of online communities. In *Digital privacy, theries, technologies and practices*, ed. Alessandro Acquisti, Stefanos Gritzalis, Costas Lambrinousakis, and Sabrina De Capitani di Vecemercati. New York: Auerbach Publications.
Le Métayer, Daniel, and Shara Monteleone. 2009. Automated consent through privacy agent: Legal requirements and technical architecture. *Computer Law Security Review* 25(2): 136–144.

Lusoli, Wainer, Margherita Bacigalupo, Francisco Lupiañez, Norberto Andrade, Shara Monteleone, and Ioannis Maghiros. 2012. *Pan-European Survey of practices, attitudes & policy preferences as regard personal identity data management*. JRC Scientific and Policy Reports, EUR 25295.

Margaryan, Anoush, Allison Littlejohn, and Gabrielle Vojt. 2011. Are digital natives a myth or reality? *Computers in Education* 56: 429–440.

Marwick, Alice, Diego Murgia-Díaz, and John Palfrey. 2010. Youth, privacy and reputation. *Berkman Center Research Publications No. 2010-5.* Harvard: Harvard University.

Mateus, Alexandre. M., and Jon. M. Peha. 2011. Quantifying global transfers of copyrighted content using BitTorrent. In *39th telecommunications policy research conference (TPRC) 2011.* Arlington: George Mason University School of Law.

Mccolm, Helen. 2011. Smart regulation: The European Commission's updated strategy. *European Journal of Risk Regulation*.

Meuwese, Anne. 2008. *Impact assessment in EU lawmaking*. The Hague: Kluwer Law International. Last accessed June 2012.

Minnesota girl alleges school privacy invasion, *CNN U.S.*, 10 Mar 2012, http://articles.cnn.com/2012-03-10/us/us_minnesota-student-privacy_1_school-counselor-school-house-gate-facebook?_s=PM:US.

Nissenbaum, Helen. 2004. Privacy as contextual integrity. *Washington Law Review* 79(1): 119–158.

Palfrey, John, and Urs Grasser. 2008. *Born digital*. New York: Basic Books.

Pascu, Corina, David Osimo, Geomina Turlea, Martin Ulbric, Yves Punie, and Jean-Claude Burgelman. 2008. Social computing – Implications for the EU innovation landscape. *Foresight* 10(1): 37–52. Emerald.

Poullet, Yves. 2010. About the E-privacy directive: Towards a third generation of data protection legislation? In *Data protection in a profiled world*, ed. Serge Gutwirth, Yves Poullet, and Paul De Hert. Dordrecht/London: Springer.

Prensky, Marc. 2001. Digital natives, digital immigrants. *On The Horizon* 9(5): 1–6. MCB University Press.

Purtova, Nadezhda. 2012. *Property rights in personal data. A European perspective*. Alphen aan den Rijn: Kluwer Law International.

Reed, C. 2010. How to make bad law: Lessons from the computing and communications sector. Queen Mary School of Law Legal Studies Research Paper No. 40/2010.

Riva, Giuseppe. 2005. The psychology of ambient intelligence: Activity, situation and presence. In *Ambient intelligence: The evolution of technology, communication and cognition towards the future of human-computer interaction*, ed. Giuseppe Riva, F. VItalaro, F. Davide, and M. Alcaniz. Amsterdam: IOS Press.

Rochelandet, Fabrice, and Silvio H. T. Tai. 2012. Do privacy laws affect the location decisions of internet firms? Evidence for privacy havens. Available: http://ssrn.com/abstract=2022160.

Rouvroy, Antoinette. 2008. Privacy, data protection, and the unprecedented challenges of ambient inteligence. *Studies in ethics, law, and technology.* Berkeley: Berkeley Electronic Press.

Shah, Nishant and Fieke Jansen. 2011. *Digital alternatives with a cause? Book one: To Be*. Bangalore: The Center for Internet and Society, available at http://www.scribd.com/nilofarh/d/65628308-Book-1-To-Be-Digital-Alternatives-With-a-Cause.

Shmidt, Aernout. 2009. Radbruch in cyberspace: About law-system quality and ICT innovation. *Masaryk University Journal of Law and Technology* 3(2): 195–218.

Solove, Daniel. 2008. *Understanding privacy*. Harvard: Harvard University Press.

Swire, Peter. 2012. Social networks, privacy, and freedom of association: Data empowerment vs. data protection. *North Carolina Law Review, 2012; Ohio State Public Law Working Paper 165; 2011 TPRC Conference.*

Tene, Omer. 2011. Privacy: The new generations. *International Data Privacy Law* 1(1): 15–27.

Thomas, Micheal. 2001. *Deconstructing digital natives. Young people and new literacy*. New York: Routledge.

Vandoninck, Sofie, Leen d'Haenens, and Veronica Donoso. 2010. Digital literacy among Flemish adolescents: How do they handle with online risks? *Communications* 35(4): 397–416.

West, Heather 2009. Is online privacy a generational issue?. *GeekDad, Wired.com*. http://www.wired.com/geekdad/2009/10/is-online-privacy-a-generational-issue/.

Wong, Rebecca. 2009. Social networking: A conceptual analysis of a data controller. *Communications Law* 14(5): 142–149.

Wong, Rebecca. 2011. Data protection: The future of privacy. *Computer Law and Security Review* 27(1): 53–57.

Chapter 6
Autonomy in ICT for Older Persons at the Crossroads Between Legal and Care Practices

Daniel Lopez Gomez, Eugenio Mantovani, and Paul De Hert

6.1 Introduction

In a context of demographic ageing, financial crisis, social and healthcare spending cuts, most of the solutions to cope with an increasing demand of long-term care entail developing different sorts of ICT platforms and systems. Technologies for ageing hold the promise to enable the older user to receive the needed care at home, to strengthen the capacity to take control over his or her life, to decide how much care he or she wants. Introduced as a way to speed up the dismantlement of the old-fashioned and expensive healthcare institutions, technologies for health are today primed to promote something traditionally disregarded, the autonomy of the aged.[1]

From the 1970s on, traditional care institutions such as nursing homes were seen as economically unsustainable and unfit to cope with the increasing demand of long-term care in a social context characterised by loosening community ties and increased individualisation. During the same period, furthermore, the moral and psychological effects on individuals, mostly elderly, populating nursing homes and other so called "total institutions"[2] begun to be criticised by post second world war civil rights movements.[3] This process of deinstitutionalisation has been characterised as

[1] For a deeper understanding of how the value of autonomy has turned into the guiding principle of active ageing policies see Alan Walker, "The Emergence and Application of Active Aging in Europe," in *Soziale Lebenslaufpolitik*, ed. Gerhard Naegele (VS Verlag für Sozialwissenschaften, 2010).

[2] Erving Goffman, *Asylums: Essays on the Social Situation of Mental Patients and Other Inmates* (New Brunswick, NJ: Aldine Transaction, 2007).

[3] See, Crossley, Nick, *Contesting Psychiatry* (Abingdon, Oxfordshire: Routledge, 2006), and Katz, Stephen, *Disciplining Old Age* (Charlottesville: University Press of Virginia, 1996).

D.L. Gomez (✉) • E. Mantovani • P. De Hert
Law, Science, Technology & Society, Vrije Universiteit Brussel, 2, Pleinlaan,
Brussel 1050, Belgium
e-mail: dlopezgo@vub.ac.be; Eugenio.Mantovani@vub.ac.be; paul.de.hert@vub.ac.be

S. Gutwirth et al. (eds.), *European Data Protection: Coming of Age*,
DOI 10.1007/978-94-007-5170-5_6,

comprised of three elementary shifts: depopulation, or the shrinking of state hospital censuses; diversion, or the deflection of potential institutional admissions to community-based service settings; and decentralisation, or the broadening of responsibility for patient care from a single service entity to multiple service entities, with an attendant fragmentation of authority.[4]

Pivotal importance is attributed to the studies of Ervin Goffman. In *Asylums: Essays on the Social Situation of Mental Patients and Other Inmates*,[5] Goffman shows how within different settings ranging from nursing houses to army barracks, mental hospitals, nunneries, and prisons human beings are confined with the purpose of re-constituting their identities as docile and dull subjects, reinforcing the chronicity of their conditions, dependency and social exclusion. Along with Michel Foucault's *Discipline and Punish*,[6] the studies of Goffman were adopted by civil rights movements, professional platforms of social workers, as well as by some psychologists who started promoting the idea that autonomy had to be respected and enforced precisely where chronicity and dependency had been normalised.[7] For the Independent Living Movement,[8] for example, the reform had to downright rethink the notion of autonomy and distinguish between on the one hand the capacity to decide and to exercise control over whatever activities are needed in order to fulfil one's desires (decisional autonomy), and, on the other hand, the capacity to physically and mentally perform these activities for oneself without assistance (executive autonomy). It is this decisional autonomy that is considered by the Independent Living Movement as the starting point of any relationship of care. By contrast, care, regardless how benevolent, had to be totally rejected insofar as it was based on a relationship in which the cared for was the passive receiver wholly defined by its handicaps, while the control of the care relationship was given to experts who knew better, with no room for a more symmetrical negotiation.[9] That was the beginning of a sea change. In time, the distinction between decisional autonomy and executive autonomy led to a remodelling of the notion of care also in the case of long-term care for older people, placing the voice and will of the human being at the centre of the care work and care policy.[10]

---

[4] Leona L Bachrach, "Deinstitutionalization: A Semantic Analysis," *Journal of Social Issues* 45, no. 3 (1989): doi:10.1111/j.1540-4560.1989.tb01562.x.

[5] Goffman, *Asylums: Essays on the Social Situation of Mental Patients and Other Inmates*.

[6] Foucault, Michel, *Discipline and Punish* (New York: Vintage Books, 1995).

[7] Bachrach, "Deinstitutionalization: A Semantic Analysis".

[8] Tom Shakespeare, "Disabled People's Self-organisation: A New Social Movement?," *Disability, Handicap & Society* 8, no. 3 (2007): doi:10.1080/02674649366780261.

[9] Tom Shakespeare, "The Social Relations of Care," in *Rethinking Social Policy*, ed. Sharon Gewirtz, John Clarke and Gail Lewis (London: Open University in association with Sage Publications, 2000).

[10] Bart J Collopy, "Autonomy in Long Term Care: Some Crucial Distinctions," *The Gerontologist* 28, no. Suppl (1988): doi:10.1093/geront/28.Suppl.10.

The emphasis put on autonomy through ICT is adroitly producing a paradigmatic change that affects traditional care too. The consent of the patient-user is evoked as the golden rule to ensure that autonomy is respected, even though consent does not automatically guarantee that autonomy is respected, particularly when the relationship of care is mediated by technological setups. The snag is that autonomy may also be undermined by ICT.

This contribution discusses two types of autonomy in ICT for older persons: autonomy in ICT for older persons as derived from the principles elaborated by legal practice on the notions of privacy and data protection; and autonomy in ICT for older persons as an achievement on account of by care-in-practice in long-term care. After contextualizing autonomy from the standpoint of law, the article draws from care-in-practice studies with the view of bringing to its real proportions the notion of autonomy and the role of consent. The tensions and overlaps of legal and care-in-practice modes of enacting the autonomy of the older people are displayed and discussed to prevent the inclusion of autonomy in ICT for older people from getting trapped either in excessive proceduralised mechanisms that may judicialize care practises or in coercive care practices that may disregard the autonomy of older people.

6.2 Autonomy: The Intersection of Law and Care Practice

The notion of autonomy has a long history and is deeply rooted in the liberal tradition since the Enlightenment, when autonomy was developed as a set of moral values of mankind and citizenship.[11] Despite its specific historical and philosophical significance, recently autonomy has been used explicitly as the value based ethics sustaining policies of long-term care and care technology development.

The discussions around the autonomy of the older people and patients in long term care situations have led to different kind of terminological distinctions.[12] For example, according to George J. Agich, autonomy can be conceived as (a) self-reliance, i.e., the capacity to provide for one's own needs; (b) personal preferences, the capacity to express your own wishes, desires and impulses and make your own decision and choices; and (c) self-assertion, the pursuit of the fulfilment of one's

[11] The notion of autonomy in the context of care has been discussed in Solveig Magnus Reindal, "Independence, Dependence, Interdependence: Some Reflections on the Subject and Personal Autonomy," *Disability & Society* 14, no. 3 (1999): doi:10.1080/09687599926190. See also, Eric L Krakauer, "Prescriptions: Autonomy, Humanism and the Purpose of Health Technology," *Theoretical Medicine and Bioethics* 19 (1998): 525–545; and Alfred I Tauber, "Historical and Philosophical Reflections on Patient Autonomy," *Health Care Analysis* 9, no. 9 (2001): doi:10.1023/A:1012901831835.

[12] Sue Davies, Sara Laker and Lorraine Ellis, "Promoting Autonomy and Independence for Older People Within Nursing Practice: A Literature Review," *Journal of Advanced Nursing* 26, no. 2 (1997): doi:10.1046/j.1365-2702.2000.00348.x.

desires and goals.[13] It is interesting to contrast these definitions with the definitions of autonomy surveyed by Gerald Dworking. He noted that autonomy had been equated to "liberty (positive and negative), dignity, integrity, individuality, independence, responsibility and self knowledge, self assertion, critical reflection, freedom from obligation, absence of external causation, and knowledge of one's own interests".[14] In both cases autonomy is a matter of principle, but as Agich said "the ethical and practical significance of autonomy ultimately rests on its presence in the world of everyday life".[15] One might notice how different understandings of the notion of autonomy come into play given a context, for example, home care, telecare, nursing house, etc. and specifically the interferences and continuities between the autonomy enacted as a legal attribute and as an empirical achievement resulting from specific care practices.

In what follows, we shall limit ourselves to illustrate the two modes of approaching autonomy only. Next paragraphs discuss autonomy in ICT for older persons from the standpoint or mode of ordering of the European legal framework on privacy and data protection. Subsequently, we are going to review the notion of autonomy from the perspective of care studies.[16]

6.2.1 A Legal Approach to Autonomy in Long-Term Care from the Right to Privacy and Data Protection Perspective

In contexts such as telecare, which include technological set ups relying on the continuous and seamless processing of persons data, the notion of the autonomy of the cared for or patient overlaps with the notion of the autonomy of citizen and the data subject. For the citizen living in democratic constitutional states, the notion of autonomy emerges as part of the right of privacy and family life; for the data subject, the legal framework on data protection applies.[17]

---

[13] George J Agich, *Dependence and Autonomy in Old Age* (Cambridge, UK; New York: Cambridge University Press, 2003).

[14] Gerald Dworkin, *The Theory and Practice of Autonomy* (Cambridge; New York: Cambridge University Press, 1988), 6.

[15] Agich, *Dependence and Autonomy in Old Age*, 11.

[16] This is not the only possible one. Other include gender studies, disability studies, STS, etc..

[17] For a comprehensive outline including social, philosophical views on privacy and data protection see Paul De Hert and Serge Gutwirth, "Privacy, Data Protection and Law Enforcement. Opacity of the Individual and Transparency of Power", in Erik Claes, Anthony Duff et al. (eds.), *Privacy and the Criminal Law* (Intersentia, Antwerp, Oxford, 2006), 61–104. Priscella Regan, *Legislating Privacy: Technology, Social Values and Public Policy* (University of North Carolina Press, 1995). Ferdinand David Schoeman, *Privacy and Social Freedom* (Cambridge University Press: Cambridge, 1992). Colin J. Bennett and Charles D. Raab, *The Governance of Privacy* (MIT Press: Cambridge, MA, 2006). Daniel J. Solove, *Understanding Privacy* (Harvard University Press, Cambridge, MA, 2008).

The right to privacy operates as a tool that embodies normative choices about the limits of power in democratic states.[18] Privacy as normative choice is the answer to a sheer political question, namely, whether and to what extent power should be limited, stopped or prohibited. This is reflected in positive law in the requirement of "necessity in a democratic state" enshrined in article 8 of the 1950 European Convention on Human Rights, which fends off interferences by public authorities and by private parties (article 8, paragraph one), unless necessary in a democratic society (article 8, paragraph two). The negative shielding function of privacy does not, however, exhaust the normativity of the right to privacy. Progressively,[19] privacy has amorphously moved to become the enabling tool to the free construction of one's personality, the projection of democratic principles into the private sphere. The normativity of the right to privacy is captured in at the point when individuals take positive action, express themselves, perform, and differ in the way they engage in constitutionally recognised relationships, sexuality, health work, culture and social life, in childhood, and also in old age.[20] The balancing of power and resistance that is inherent in the right to privacy enables autonomy as the right to forge individualised relationships. This, *in nuce*, is the autonomy privacy protects and promotes also in contexts of care.

As opposed to the normative, eminently positive, role of privacy, data protection comes into play as an essentially negative, transparency tool to ensure that personal data are processed in ways that make it unlikely that personal integrity and privacy are infringed or invaded.[21] More explicitly, while privacy responds to the political need to limit, stop or prohibit, data protection law answers to the social need to control and challenge the legitimate uses of power,[22] providing specific safeguards

---

See also FP7-SCIENCE-IN-SOCIETY-2009-1 SiS-2009-1.1.2.1 Privacy and emerging fields of science and technology: ethical, social and legal aspects – WP 1 – Current legal, socio-economic and ethical approaches to privacy and technology, *Discussion Paper,* authored by Michael Friedewald and Philip Schütz (Fraunhofer ISI), Serge Gutwirth, Raphael Gellert and Rocco Bellanova (VUB), David Wright (Trilateral Research & Consulting), Emilio Mordini and Silvia Venier (CSSC), 2010.

[18] De Hert & Gutwirth, "Privacy, data protection and law enforcement. Opacity of the individual and transparency of power", 70.

[19] Notably through the case law of the European Court of Human Rights: ECtHR judgment of 29 April 2002, Pretty v. United Kingdom, appl. no. 2346/02, para. 61: "Although no previous case has established as such any right to self-determination as being contained in Article 8 of the Convention, the Court considers that the notion of personal autonomy is an important principle underlying the interpretation of its guarantees." ECtHR judgment of 12 January 2010, Gillan and Quinton v. the United Kingdom, appl. no. 4158/05, para. 61; ECtHR judgment of 27 April 2010, Ciubotaru v. Moldova, appl. no. 27138/04, para. 49.

[20] Article 25 of the 2000 EU Charter of Fundamental Rights, The Right of the Elderly. "The Union recognises and respects the rights of the elderly to lead a life of dignity and independence and to participate in social and cultural life." In general, see Gutwirth, Serge, *Privacy and the Information Age* (Lanham: Rowman & Littlefield, 2002).

[21] De Hert & Gutwirth, "Privacy, data protection and law enforcement. Opacity of the individual and transparency of power", p. 76.

[22] De Hert & Gutwirth, "Privacy, data protection and law enforcement. Opacity of the individual and transparency of power", ibid.

and promoting accountability by government and private record-holders. The difference, accredited formally by the insertion of a distinct provision at the levels of constitutional and public law,[23] is substantial: data protection protects values that are not at the core of privacy.[24] The core content of the right to data protection is to ensure that the processing of information relating to a person remains fair and lawful. Accordingly, the linchpin of data protection is not found in a "right claim to…" but in a principle, data minimisation, and a series of quintessential conditions of fair processing, including legitimacy, proportionality, and also consent.

Privacy (article 7 of the EU Charter of Fundamental Rights) and data protection (article 8 of the EU Charter of Fundamental Rights) are therefore two different rights. And yet, they are closely linked. The relationships and reciprocal contaminations between these two important rights for the protection of older persons in the information society, however, have not been uncomplicated. The expression "danger of proceduralisation" refers to a shift in the right to private life from a prohibitive (or opacity) logic into a channelling one, into a transparency-promoting vehicle.[25] This means that virtually any data processing activity is legitimate as long as it fulfils the requirements of data protection, notably through the giving of consent. As a consequence, there are more areas in which opaque limits are simply put off; there are instead numerous possibilities to trade off privacy and render processing legitimate.[26]

One area in which this *proceduralisation* is particularly apparent is ICT for older persons. In this area, the possibilities of trading off privacy and render processing legitimate are expanded through the latch of individual consent. And the adduced justification for the prime role of consent as legitimate basis for lawful data processing is that it expresses and promotes autonomy. The growing importance endowed on consent as benchmark for the respect for individual autonomy in the context of ICT for older persons is problematic.

The use of consent occurs at a time of significant technological and social changes.[27] Technically, new technologies capable of recognising traces left behind by human beings create an unprecedented abundance of new data, such as key-coded

[23] Article 8 of the 2000 Charter of Fundamental Rights of the European Union and the data protection Directive 95/46/EC. The right to privacy is enshrined in articke 7 of the EU Charter.

[24] For a criticism of the recent case law of the European Court of Justice and of the European Court of Human Rights in this are see Gloria Gonzalez Fuster and Raphaël Gellert "The fundamental right of data protection in the European Union: in search of an uncharted right." *International Review of Law, Computers & Technology* 26, no. 1 (2012): doi: 10.1080/13600869.2012.646798.

[25] De Hert & Gutwirth, "Privacy, data protection and law enforcement. Opacity of the individual and transparency of power", 87.

[26] De Hert & Gutwirth, "Privacy, data protection and law enforcement. Opacity of the individual and transparency of power", Ibid.

[27] Article 29 Data Protection Working Party, *The Future of Privacy. Joint contribution to the Consultation of the European Commission on the Legal Framework for the Fundamental Right to Protection of Personal Data*, Adopted on 01 December 2009, 02356/09/EN, WP 168; see also Opinion 15/2011 on Consent, 13 July 2011, WP 187, and the recent European Group on Ethics in Science and New Technologies (EGE), *Ethics of Information and Communication Technologies*, 22.02.2012, No. 26.

data, and location data. Profiling techniques make it possible to generate new personal data which are not those which the data subject has communicated to the controller. At societal level, people seem to be growingly careless with their data.[28] This may also due to the fact that in contexts of unbalanced relations of power, notably in the workplace and health context, business models and consumer vendor relationships, often the individual is outstripped of the ability to make informed decisions about data processing.

The foregoing holds particularly true in the context of ICT for ageing.[29] There are at least three levels of interaction of older persons with ICT that should give pause. First, many older individuals (more, as compared to younger cohorts) who suffer from chronic illness may experience problems with reduced capacity. For such individuals, the capacity to give consent will be accorded according to the local legal position. Often this will be in the form of a guardian.[30] This situation can be complicated where capacity fluctuates throughout the life of individuals with chronic illness. With persons with diabetes, for instance, one can foresee problems with patients suffering from long-term complications or short-term hypoglycaemic episodes that potentially interact on a 24 h basis with an e-Health based platform. Such a situation could see an individual giving consent during a period in which they technically did not possess the capacity to give consent. One could envisage an individual giving consent for his or her data to be shared with external third parties or for further types of his health data to be collected than he had previously agreed.[31]

Second, as suggested above, where the power of each party to an agreement is far from equal it can sometimes be a fiction to speak of autonomy because the party concerned has given his or her consent. This can be especially true if individuals are in positions of dependency. More explicitly, part of the problem of unbalanced relations in the arena of care provision occurs because individuals do not really have an alternative choice. They often face a choice of obtaining care, or to do without.[32] This instils a resounding power asymmetry into the relationship between user/patient and care provider. Bluntly put, in order to provide as high a level of autonomy,

---

[28] According to a recent Eurobarometer (IP/11/742), 70 % of Europeans are concerned that their personal data may be misused. They are worried that companies may be passing on their data to other companies without their permission. However, 74 % of Europeans think that disclosing personal data is increasingly part of modern life.

[29] Emilio Mordini, and Paul De Hert (eds), *Ageing and Invisibility* (IOS Press: The Netherlands, 2010).

[30] For a detailed overview and discussion see P. Bartlett, O. Lewis, and Oliver Thorold, *Mental Disability and the European Convention on Human Rights* (Martinus Nijhoff, Leiden, 2007), especially chapter 5. See also J.V. McHale, "Mental Incapacity: Some Proposals for Legislative Reform", *Journal of Medical Ethics*, 24, (1998): doi:10.1136/jme.24.5.322.

[31] P. Quinn, Mantovani, P. De Hert, "Ethical Issues", Internal Document, Deliverable 9.1 Remote Accessibility to Diabetes Management and Therapy in Operational healthcare Networks. *REACTION* (FP7, GA. 248590).

[32] P. De Hert, and E. Mantovani."On Consent". E. Mordini, & Paul De Hert, *Ageing and Invisibility,* 131–142.

it should be always possible to refuse e-care and live, age, heal or die *outside* the information society.

Third, and last, ageing persons are, on average, less IT savvy than younger generations. The often heard counter claim is that ICT natives will know full well how to deal with ICT and to navigate the associated risks, "when they are 64". Skills acquisition, however, also depends on the pace of technological development. The latter "outpaces" learning ability of older people, so even if they make the effort to catch up with new technologies and learn the use/adapt to a new reality, these technologies become out-dated quite rapidly, leaving an amount of people stuck to a previous reality that might not be functional any longer. Younger generations might have the motivation to follow trends, or the capacity, the eagerness, to stay in touch with anything new. But, what about older people? Can they keep up with new "gadgets"? Must they? Is there an end to it – where daily activities with ICT in place become a routine and one is, at last, "free" from learning?[33]

The foregoing suggest that when considering the introduction of modern technologies to support older persons, one should consider the value of autonomy both as a principle, as derived from the right to privacy, and also as a practical arrangement, which emerges from the framework of data protection. We should not content ourselves with the respect of the abstract reasonable middle-aged man. In particular, consent should not be used as short cut to legitimising any practice of ICT for older persons. There is also room, in the law, for learning from and adjusting to the realities in which older persons age in highly technological societies. One of such learning opportunities is explored below. The goal is to open up the black box of autonomy and bring into light the different and conflicting modes of enacting the autonomy of the older people in care contexts.

6.2.2 Autonomy in Long-Term Care from an Ethics of Care Perspective

According to a care-in-practice perspective, the main problem with the notion of autonomy is that it involves a view of the subject as coherent and independent that usually hardly fits with the reality of long-term care, where individuals need support. As Agich pointed out, this ideal of autonomy produces a tension between "independence versus dependence and capacities associated with agency versus functional frailties".[34] What Agich suggests shifts the focus of attention from the notion of autonomy to its counterpart, the notion dependency and the values

[33] Mordini and De Hert, *Ageing and Invisibility*.

[34] Agich, *Dependence and Autonomy in Old Age*, 1.

associated with it. Despite the multiple nuances of the notion of dependency,[35] the dominant narrative considers autonomy as the positive value that must be fostered and pursued only, whereas dependency is regarded as a negative state that must be alleviated.

Since autonomy is a dominant value and dependence is considered a kind of handicap or failure, using the idea of autonomy in long-term care situations without questioning it might reinforce and legitimize harmful prejudices and situations.[36] This notion of autonomy as individual in-dependence is a projection of the standards of middle-aged behaviour, functioning as a tacit norm projected onto older people. This might produce negative attitudes towards old age, especially against disabled elders, and generate frustration among ageing individuals who do not comply with this tacit norm of staying active and independent.

There is another problem with the idea of autonomy as independence. Coined as a right that must be preserved, the ethical discussion concerning long-term care situations tends to be approached in adversarial, agonistic, and categorical terms. This has important effects for the organisation of care because the preservation of the autonomy of the person may lead to transform the relation of care into a relation between adversaries, with the carers who intend to reduce the autonomy of the older person on one side, and the elderly individual striving to keep it, on the other.[37] As Jeannette Pols has shown in her ethnographic study of mental health institutions,[38] the mode of ordering of law and care in practice interfere with each other in the specific setting resulting in the emergence of different contextual *normativities* on the definition of 'good care' and of patients' autonomy. The autonomy of the client can be defined in terms moral principles that must be respected and pursued as way to give a good care – as in the case of rehabilitation, in which the relation of lawyer and client is adopted as ideal also for a caring relation between nurse and patient.

---

[35] There are different sorts of dependencies: life-cycle dependency; physical and psychological dependency, political dependency, economic and financial dependency and structural dependency. Some of these dependencies might be age-related ill-health conditions; they can also be understood as individual attributes or as the result of social factors such as the pension policies or residential care. See Nancy Fraser and Linda Gordon, "A Genealogy of Dependency: Tracing a Keyword of the U.S. Welfare State," *Signs* 19, no. 2 (1994): 309–336; and Collopy. "Autonomy in Long Term Care: Some Crucial Distinctions."

[36] For an interesting discussion concerning the side-effects and also undesired results of turning autonomy into the guiding value of ageing policies see: Larry Polivka and Harry R Moody, "A Debate on the Ethics of Aging: Does the Concept of Autonomy Provide a Sufficient Framework for Aging Policy?," *Journal of Aging and Identity* 6, no. 4 (2001): doi:10.1023/A:1012949410014.

[37] See, Agich, George J. *Dependence and Autonomy in Old Age.* Cambridge, UK ; New York: Cambridge University Press, 2003. Jeannette Pols, "Enforcing Patient Rights or Improving Care? The Interference of Two Modes of Doing Good in Mental Health Care," *Sociology of Health & Illness* 25, no. 4 (2003): doi:10.1111/1467-9566.00349.

[38] Jeannette Pols, "Enforcing Patient Rights or Improving Care? The Interference of Two Modes of Doing Good in Mental Health Care," *Sociology of Health & Illness* 25, no. 4 (2003): doi:10.1111/1467-9566.00349.

Whereas in situations of compulsory care or in which the practice of care entails some sort of coercion, the *normativities* regarding the good care and autonomy of the patient coming from the legal and care practice can collide.

In this respect, it is worth learning from gender studies and the debate on autonomy and the 'ethic of care' approach in particular.[39] From that perspective it is not possible to dignify life in contexts of long-term care if dependences are seen as a denigration of the person instead of the source of solidarity and humanity. As Kittay stated, "the emphasis on independence extols an idealisation that is a mere fiction, not only for people with disability, but for all of us. The emphasis on choice leaves out many people with disabilities for whom making choices is problematic as their cognitive function may be seriously impaired. And the denigration of care and dependency tends toward an attitude that makes the work and value of the carers invisible, thus creating one oppression in the effort to alleviate another".[40] In contrast with an approach based on autonomy as independence, gender studies define care as the ability of a human being to give and to receive care and consider care at the same level of the capacity for reason and to choose.

6.3 From Legal Practice to Care Practice: Or How to Align Different Autonomies[41]

Drawing on the debates on the ethics of care and care studies, on one side, and on the right to privacy, on the other side, we can consider autonomy as embodied and enacted in diverse engagements with technologies, persons, institutions and spaces. Autonomy is only possible in relation with others and thus there are multiple forms of being autonomous. For example, regarding new technologies of care, López and Domènech[42] and Willems[43] have shown that gaining autonomy is sometimes associated

[39] See for example, Martha Holstein and Phyllis Mitzen, *Ethics in Community-based Elder Care* (New York: Springer, 2001). Liz Lloyd, "Mortality and Morality: Ageing and the Ethics of Care," *Ageing & Society* 24, no. 02 (2004): doi:10.1017/S0144686X03001648. Michael Fine and Caroline Glendinning, "Dependence, Independence or Inter-dependence? Revisiting the Concepts of 'care' and 'dependency'," *Ageing & Society* 25, no. 04 (2005): doi:10.1017/S0144686X05003600. Marian A Verkerk, "The Care Perspective and Autonomy," *Medicine, Health Care and Philosophy* 4, no. 3 (2006): doi:10.1023/A:1012048907443.

[40] Eva Kittay, "The Ethics of Care, Dependence, and Disability," *Ratio Juris* 24, no. 1 (2011): doi:10.1111/j.1467-9337.2010.00473.x.

[41] This section is partially drawn on the etnographic studies of different telecare technologies: first generation telecare systems (social alarm), second generation telecare systems (social alarms with domestic senesors), a domestic telemedicine technology to monitor health and wellbeing at home and a social network to support caregivers. See, Maggie Mort et al., *EFORTT: Ethical Frameworks for Telecare Technologies for Older People at Home (FP7 GA. 217787)* (Lancaster: University of Lancaster, 2011).

[42] Daniel López and Miquel Domènech, "Embodying Autonomy in a Home Telecare Service," *The Sociological Review* 56, no. s2 (2009): doi:10.1111/j.1467-954X.2009.00822.x.

[43] Willems, "Managing One's Body Using Self-management Techniques: Practicing Autonomy," *Theoretical Medicine and Bioethics* 21, no. 1 (2000): 23–38.

with an active involvement in monitoring systems as a way to control the user's body and the care setting in which the patient and user is inserted, i.e. becoming a manager of your health; in other cases, autonomy is achieved the other way round, through a misuse or non-use of these systems. This is a very important ethical issue that must be taken into account in any technology development: the fact that technology might be designed to enhance the autonomy of their users does not necessarily mean that this technology is going to be appropriated by users seeking for autonomy or that this technology is going to actually increase their autonomy. Autonomy is the result of diverse factors and can be achieved very differently.[44]

The capacity to act, choose and desire emerges within engagements with others, on which we depend. Autonomy thus increases and decreases also within these engagements.[45] For example, according to the Independent Living Movement, mentioned above, in order to get more autonomy the disable person must be engaged with technologies, care-givers and spatial and temporal configurations in a way that the locus of control of certain decisions must be on the end-user, whereas the locus of execution of certain activities must be on technologies and/or personal assistants.[46] In other cases, fostering autonomy might entail a completely different distribution of dependencies. For example, in the case of people with severe chronic diseases with some sort of medical monitoring system, autonomy is achieved when the person is engaged with the e-health device and caregivers and relatives in such a way that the locus of control of the monitoring activity is delegated to the machine or the nurse at the other end of the line in such a way that he doesn't need to think about his illness during the whole day and his/her life is not defined only by this problem. In fact, one of the risks of home telemedicine devices is that some users can reject them because they feel their home is institutionalised, that it becomes a hospital.[47] In both cases, as agency is distributed according to the manner in which these engagement with technologies, spaces, persons, times are arranged, autonomy has not to do with removing dependencies but with attuning them according to effects that they produce on the people involved.[48] Consequently, autonomy cannot be understood as the materialisation of a pre-defined set of attributes associated to an essential identity (normally the ones associated with the middle-aged white non-disabled man). Autonomy on the contrary entails making sense of the dependencies,

---

[44] Rita Struhkamp, Annemarie Mol and Tsjalling Swierstra, "Dealing with In/dependence: Doctoring in Physical Rehabilitation Practice," *Science Technology & Human Values* 34, no. 1 (2009): doi:10.1177/0162243907312954.

[45] Maggie Mort *and others*, *Ageing, Technology and Home Care: New Actors, New Responsabilities* (TRANSVALOR Presses des MINES, 2008).

[46] Stefano Goodman, "Independent Living: A Disabled Man and His Personal Assistants," *The Guardian* (2009).

[47] Daniel López and Tomás Sánchez-Criado, "Dwelling the Telecare Home: Place, Location and Habitality," *Space and Culture* 12, no. 3 (2009): 343–358.

[48] Christine Milligan, Celia Roberts and Maggie Mort, "Telecare and Older People: Who Cares Where?," *Social Science & Medicine (1982)* 72, no. 3 (2011): doi:10.1016/j.socscimed.2010.08.014; and, López & Domènech, "Embodying Autonomy in a Home Telecare Service".

engaging with them to steer our life. This duty of being autonomous can be enacted in multiple forms and through legal procedures, technological means and care practices.[49]

6.4 Conclusions

We are engaged with others and therefore dependent on them. These dependencies define us as active agents with preferences and desires, they must not be understood as obstacles to be autonomous.[50] Our capacity to act, think and choose is the product of our dependencies and attachments. Any intervention that affects the latters produces changes in the former. But this understanding of autonomy does not undermine the right to privacy. On the contrary, it emphasises the necessity to protect these dependencies and attachments from disruptive and arbitrary changes.

That is the reason why the autonomy of the older people shouldn't be reduced to giving consent through a simple standard procedure. For example, in the case of a telecare system, the aged person is the one who is informed and gives consent, signs the contract with the service and is comprised by it. But it is not a smooth and mellow path. Even in such a technological mediated care service, its functioning depends on the capacity to engage others beyond the end-users. The decision of getting a telecare service is rarely individual, there are others involved who are already taking care of the person and have a role in this decision. Even though the asking/giving consent process draws the will of the aged-person from the intermingled care relations in which the aged person is embedded to turns the decision of getting the service into a reflexive and autonomous decision, the service does not aim to throw out these other actors who take care of the aged-person from the decision-making process. On the contrary, even though they can blur and mess the consent of the aged person with their own expectations and needs, they must be involved to work out the whole process and improve the telecare work.[51]

Reinforcing the autonomy of the older user does not necessarily imply to isolate him or her from the other actors involved in the caregiving work. On the contrary, it

[49] See for example Myriam Winance, "Being Normally Different? Changes to Normalization Processes: From Alignment to Work on the Norm," *Disability & Society* 22, no. 6 (2007): doi:10.1080/09687590701560261; Irene Olaussen, "Disability, Technology & Politics: The Entangled Experience of Being Hard of Hearing." (University of Oslo, Oslo, 2010); and Ingunn Moser, "Disability and the Promises of Technology: Technology, Subjectivity and Embodiment Within An Order of the Normal," *Information, Communication & Society* 9, no. 3 (2006): doi:10.1080/13691180600751348.

[50] For a discussion on the redefinition of dependency see, Eva Feder Kittay, Bruce Jennings and Angela A Wasunna, "Dependency, Difference and the Global Ethic of Longterm Care," *Journal of Political Philosophy* 13, no. 4 (2005): doi:10.1111/j.1467-9760.2005.00232.x.

[51] Giorgos Koumanakos. "Discussion on the notion of consent of older citizens in situations of dependency", Internal Document, Deliverable 2.2. *VALUE AGEING* (FP7, GA. 251686)

entails to involve them in the decision-making process while protecting the dependencies and attachment that make the user capable of making such a decision from undesired intromissions. Which means that the autonomy of the older people must enacted differently by the legal practice of consent and by the caring practices but aligned to improve the quality of care. The consent procedure intents to prevent the practical arrangements that gives the user his or her capacity to act and decided from being threatened by third parties while at the same time this practical arrangements are modified by adding and taking away elements to enhance his or her autonomy.

Acknowledgments This contribution is based on the work completed in the project "VALUE AGEING", funded by the European Commission (FP7 Marie Curie Industry-Academia Partnerships and Pathways Action). The authors wish to thank the researchers involved in the project, the organisation of the CPDP2012 conference and the reviewers for their collaboration, insights and helpful comments.

References

Agich, George J. 2003. *Dependence and autonomy in old age*. Cambridge/New York: Cambridge University Press.

Bachrach, Leona L. 1989. Deinstitutionalization: A semantic analysis. *Journal of Social Issues* 45(3): 161–171. doi:10.1111/j.1540-4560.1989.tb01562.x.

Bartlett, P., O. Lewis, and Oliver Thorold. 2007. *Mental disability and the European convention on human rights*. Leiden: Martinus Nijhoff.

Bennett, Colin J., and Charles D. Raab. 2006. *The governance of privacy*. Cambridge, MA: MIT Press.

Collopy, Bart J. 1988. Autonomy in long term care: Some crucial distinctions. *The Gerontologist* 28(Suppl): 10–17. doi:10.1093/geront/28.Suppl.10.

Crossley, Nick. 2006. *Contesting psychiatry*. Abingdon: Routledge.

Davies, Sue, Sara Laker, and Lorraine Ellis. 1997. Promoting autonomy and independence for older people within nursing practice: A literature review. *Journal of Advanced Nursing* 26(2): 408–417. doi:10.1046/j.1365-2702.2000.00348.x.

De Hert, Paul, and Serge De Gutwirth. 2006. Privacy, data protection and law enforcement. Opacity of the individual and transparency of power. In *Privacy and the criminal law*, ed. Erik Claes, Anthony Duff, et al., 61–104. Antwerp/Oxford: Intersentia.

Dworkin, Gerald. 1988. *The theory and practice of autonomy*. Cambridge/New York: Cambridge University Press.

Fine, Michael, and Caroline Glendinning. 2005. Dependence, independence or inter-dependence? Revisiting the concepts of 'care' and 'dependency'. *Ageing and Society* 25(04): 601–621. doi:10.1017/S0144686X05003600.

Foucault, Michel. 1995. *Discipline and punish*. New York: Vintage Books.

Fraser, Nancy, and Linda Gordon. 1994. A genealogy of dependency: Tracing a keyword of the U.S. Welfare State. *Signs* 19(2): 309–336.

Friedewald, Michael and Philip Schütz (Fraunhofer ISI), Serge Gutwirth, Raphael Gellert and Rocco Bellanova (VUB), David Wright (Trilateral Research & Consulting), Emilio Mordini and Silvia Venier (CSSC). 2010. Privacy and emerging fields of science and technology: Ethical, social and legal aspects – WP 1 – Current legal, socio-economic and ethical approaches to privacy and technology. Discussion Paper, FP7-SCIENCE-IN-SOCIETY-2009-1 SiS-2009-1.1.2.1.

Goffman, Erving. 2007. *Asylums: Essays on the social situation of mental patients and other inmates*. Reprint ed. New Brunswick: Aldine Transaction.
Gonzalez Fuster, Gloria, and Raphaël Gellert. 2012. The fundamental right of data protection in the European Union: In search of an uncharted right. *International Review of Law, Computers and Technology* 26(1): 73–82. doi:10.1080/13600869.2012.646798.
Goodman, Stefano. 2009. Independent living: A disabled man and his personal assistants. *The Guardian*, 11 Nov 2009.
Gutwirth, Serge. 2002. *Privacy and the information age*. Lanham: Rowman & Littlefield.
Holstein, Martha, and Phyllis Mitzen. 2001. *Ethics in community-based elder care*. New York: Springer.
Katz, Stephen. 1996. *Disciplining old age*. Charlottesville: University Press of Virginia.
Kittay, Eva. 2011. The ethics of care, dependence, and disability. *Ratio Juris* 24(1): 49–58. doi:10.1111/j.1467-9337.2010.00473.x.
Kittay, Eva Feder, Bruce Jennings, and Angela A. Wasunna. 2005. Dependency, difference and the global ethic of longterm care. *Journal of Political Philosophy* 13(4): 443–469. doi:10.1111/j.1467-9760.2005.00232.x.
Krakauer, Eric L. 1998. Prescriptions: Autonomy, humanism and the purpose of health technology. *Theoretical Medicine and Bioethics* 19: 525–545.
Lloyd, Liz. 2004. Mortality and morality: Ageing and the ethics of care. *Ageing and Society* 24(02): 235–256. doi:10.1017/S0144686X03001648.
López, Daniel, and Miquel Domènech. 2009. Embodying autonomy in a home telecare service. *The Sociological Review* 56(s2): 181–195. doi:10.1111/j.1467-954X.2009.00822.x.
López, Daniel, and Tomás Sánchez-Criado. 2009. Dwelling the telecare home: Place, location and habitality. *Space and Culture* 12(3): 343–358.
McHale, J.V. 1998. Mental incapacity: Some proposals for legislative reform. *Journal of Medical Ethics* 24: 322–327.
Milligan, Christine, Celia Roberts, and Maggie Mort. 2011. Telecare and older people: Who cares where? *Social Science & Medicine (1982)* 72(3): 347–354. doi:10.1016/j.socscimed.2010.08.014.
Mordini, Emilio, and Paul De Hert (eds.). 2010. *Ageing and invisibility*. Amsterdam: Ios Press.
Mort, M., C. Milligan, C. Roberts, and I. Moser. 2008. *Ageing, technology and home care: New actors, new responsibilities*. Paris: Transvalor Presses des Mines.
Moser, Ingunn. 2006. Disability and the promises of technology: Technology, subjectivity and embodiment within an order of the normal. *Information, Communication & Society* 9(3): 373–395. doi:10.1080/13691180600751348.
Olaussen, Irene. 2010. *Disability, technology and politics: The entangled experience of being hard of hearing*. Oslo: University of Oslo.
Polivka, Larry, and Harry R. Moody. 2001. A debate on the ethics of aging: Does the concept of autonomy provide a sufficient framework for aging policy? *Journal of Aging and Identity* 6(4): 223–237. doi:10.1023/A:1012949410014.
Pols, Jeannette. 2003. Enforcing patient rights or improving care? The interference of two modes of doing good in mental health care. *Sociology of Health & Illness* 25(4): 320–347. doi:10.1111/1467-9566.00349.
Quinn, Paul, E. Mantovani, and P. De Hert. *Ethical Issues*, Internal Document, Deliverable 9.1 Remote Accessibility to Diabetes Management and Therapy in Operational healthcare Networks. REACTION (FP7, GA. 248590)
Regan, Priscella. 1995. *Legislating privacy: Technology, social values and public policy*. Chapel Hill: University of North Carolina Press.
Reindal, Solveig Magnus. 1999. Independence, dependence, interdependence: Some reflections on the subject and personal autonomy. *Disability and Society* 14(3): 353–367. doi:10.1080/09687599926190.
Schoeman, Ferdinand David. 1992. *Privacy and social freedom*. Cambridge: Cambridge University Press.

Shakespeare, Tom. 2000. The social relations of care. In *Rethinking social policy*, ed. Sharon Gewirtz, John Clarke, and Gail Lewis. London: Open University in association with Sage Publications.

Shakespeare, Tom. 2007. Disabled people's self-organisation: A new social movement? *Disability, Handicap & Society* 8(3): 249–264. doi:10.1080/02674649366780261.

Solove, Daniel J. 2008. *Understanding privacy*. Cambridge, MA: Harvard University Press.

Struhkamp, Rita, Annemarie Mol, and Tsjalling Swierstra. 2009. Dealing with in/dependence: Doctoring in physical rehabilitation practice. *Science Technology and Human Values* 34(1): 3–5. doi:10.1177/0162243907312954.

Tauber, Alfred I. 2001. Historical and philosophical reflections on patient autonomy. *Health Care Analysis* 9(3): 299–319. doi:10.1023/A:1012901831835.

Verkerk, Marian A. 2006. The care perspective and autonomy. *Medicine, Health Care and Philosophy* 4(3): 289–294. doi:10.1023/A:1012048907443.

Walker, Alan. 2010. The emergence and application of active aging in Europe. In *Soziale lebenslaufpolitik*, ed. Gerhard Naegele. Wiesbaden: VS Verlag für Sozialwissenschaften.

Willems, Dick. 2000. Managing one's body using self-management techniques: Practicing autonomy. *Theoretical Medicine and Bioethics* 21(1): 23–38.

Winance, Myriam. 2007. Being normally different? Changes to normalization processes: From alignment to work on the norm. *Disability and Society* 22(6): 625–638. doi:10.1080/09687590701560261.

Chapter 7
Ethical Implications of Technologies That "Support" Ageing with Dementia at Home

Unai Díaz-Orueta and Elena Urdaneta

7.1 Introduction

The progressive introduction of Assistive Technologies in our society has posed the threat of leaving behind those who cannot keep easily updated with the demands imposed by a fast evolving information society. In the latest years, the investment from European Commission to overcome the establishment of a digital divide between technology and those target populations that may be at a higher risk of being left behind (older people and disabled), has been high and several projects integrating ICTs in lives of older and people with disabilities haven been financed. This has led to numerous progresses from the technological point of view (such as the Open URC Consortium – www.openurc.org). However, when it comes to defend ICTs integration in older people's lives, and how technology has actually influenced older people's daily life, doubts persist on (1) whether the developed technologies do actually fulfil older users' wishes and needs; and (2) whether the developed technologies for older users respect main ethical principles as much as they should. On a relatively recent paper drew on a project on the integration of technology in older people's lives, Diaz, Garcia and Urdaneta (2010) found that (1) older people do not want to rely on third parties, they want to have control of their devices (*control of the environment*), which is in agreement with Theory of Planned Behavior (Ajzen 1991; Phang et al. 2006); (2) older people do not want technology that make them more dependent (*preservation of autonomy*) (Consolvo et al. 2004; van Veldhoven et al. 2008); and (3) older people do not want to buy new technologies, but to rely on existing devices and develop new uses (*optimization of resources and costs*)

U. Díaz-Orueta, Ph.D. (✉) • E. Urdaneta, Ph.D.
Fundación Instituto Gerontológico Matia – INGEMA,
1-3, Paseo de Mikeletegi, 20009 Donostia-San Sebastian, Spain
e-mail: undiaz@gmail.com; elena.urdaneta@ingema.es.

S. Gutwirth et al. (eds.), *European Data Protection: Coming of Age*,
DOI 10.1007/978-94-007-5170-5_7, © Springer Science+Business Media Dordrecht 2013

(Cimperman 2010; Coughlin et al. 2007). When dealing with people with dementia, special considerations need to be taken into account when it comes to integrating ICTs in the daily environment of people with dementia. In the following sections we will try to address the main ethical principles observed in research and how preservation of these principles may enter in conflict with the goals of ICT development when dealing with a target population such as older people with dementia, for whom the balance between technological progress and users' rights' preservation is more delicate.

7.2 Main Ethical Principles in Research and Their Appliance to Research with Older Users with Dementia

We try to present the main ethical principles when conducting research, as collected in the European Directives 95/46/EC (European Union 1995) and 97/66/EC (European Union 1995), together with reflections on how they should be applied when developing research with older users, based on the work from Pauwels (2007) and our country-specific experience on the observance and fulfillment of Spanish decree 223 (Royal Decree 2004), and Spanish Data Protection Law (Spanish Organic Law 1999).

- **Privacy**: Technologies that monitor a person's activity or lifestyle raise privacy and dignity concerns. Specially with older people, who may be in a vulnerable position of less understanding about the risk to privacy loss derived from using particular technologies, it should be clearly specified to them, with easy words, what data are collected; which type of processing, interpretation and presentation are permitted; and who should have access to the information collected. Moreover, it is expected that most of the older adults with dementia will not fully comprehend to what extent autonomous ICT collect and transmit data, and by whom these date can be accessed, so special caution must be paid when explaining this aspects to them. This effort is being specially put, for example, in the BEDMOND project is (www.bedmond.eu), whose objective is to develop an ICT-based system for an early detection of Alzheimer's disease and other neurodegenerative diseases, specifically designed for elderly people while living at home. In this project, the information necessary to this evaluation will be gathered by a non-intrusive sensor network installed at the user's home to track the elderly behaviour. In the evaluations being held by our team (www.ingema.es), evaluators are putting special emphasis on the nature of the sensors and consent form description (explaining it to the older person as many times as necessary) prior to the subsequent installation of sensors in users' homes. In this project, after being presented with the proper information, participants (in initial stages of a dementia) have appeared to be willing to sacrifice their privacy if this is something that can be helpful in the future for other people in their same circumstances.
- **Proportionality**: The level of intervention should be restricted to what is really necessary for the situation. If you will obtain the same information from a 2-h

individual interview with the person and from a 1-h focus group intervention, you should probably go for the second option. Of course, often it is not the choice of the older persons but their carers', who will be the ones choosing or specifying the required technology. However, if you can derive user requirements for technology use in 10 key questions about the person's experience with technology rather than in a 200 items questionnaire filled with sensitive information about health, cognition, lifestyle and political orientation, it is quite obvious that you should direct your efforts to the implementation of the first option. In VITAL project (www.ist-vital.org), there was a problem with the extension of the individual interviews in the first stage. Interviews led to large amounts of information (including questions about users' quality of life) that appeared to be irrelevant to assess the adequacy of the technology to the users' needs. Hence, based on the principle of proportionality, it was decided that, in final evaluations, individual evaluations would be avoided; instead, focus groups would be performed targeting questions specifically relevant for the project stage; this led to a successful outcome of the project without forcing the users' to reveal more information than necessary about themselves.

- **Purposefulness**: Information should not be gathered unless it has a clearly specified purpose that is related to the needs being addressed. So, for example, if you plan to fill an demented older person's home with behavioural recognition cameras to monitor disruptive behavioural patterns, that should be justified by the benefits of such an intrusive means to collect information (recording of image, voice, private conversations…), and by the absence of less intrusive alternatives (i.e. such as the use of RFID tags, as the ones that are being implemented in BEDMOND project). If you cannot justify that using cameras is proportionate and either the unique or the most beneficial way to collect that information, or if the same goal can be fulfilled with less intrusiveness, the application of this principle should lead you to think on other alternatives. In HERMES project (HERMES Consortium 2008; Jiang et al. 2008), in which specific fragments of audio and video needed to be recorded on a PDA to push older users' episodic memory while and after having conversations with others, it was agreed to set different levels of privacy to ensure both the protection of privacy of third parties and purposefulness of the recordings. Hence, the older person could go outside with the HERMES PDA and then, the system could act according to the following privacy levels: (a) level 0: the persons that talk to the user outside home give their consent for being recorded in audio and video; when the faces and voices of these persons are recognized by HERMES, the system records them; (b) level 1: the persons that talk to the user outside home give their consent for being recorded in audio but not in video; when these persons talk, HERMES recognizes their voices and records them in audio but not in video; and (c) level 2: the persons that usually talk to the user outside home do not give their consent for being recorded; HERMES does not record anything, so the user needs to take some notes in the PDA after the conversation.
- **Justice**: Equal share and fairness, avoiding exploitation and abuse of participants. In practical terms, this means that not everything is permitted when implementing

ICTs in the home of a person with dementia just because you assume that he will not be conscious or will not remember all the details about the technology you want to implement.

- **Respect**: As a researcher, one cannot rely on the demented person's cognitive problems to override or forget their right to be informed about the study, the right to freely decide whether to participate in a study, and the right to withdraw at any time without penalty. Article 6 of the Universal Declaration of Human Rights (United Nations 1948) recognizes everyone as a person before the law, and article 27 states that "everyone has the right freely to participate in the cultural life of the community, to enjoy the arts and to share in scientific advancement and its benefits." This participation and enjoyment cannot be forced or obtained at all costs. On the contrary, people with dementia and their capacity to make decisions need to be respected, and only a rigorous evaluation of their competence may determine whether the person has lost this capacity.
- **Beneficence**: It implies balancing the benefits of treatment against the risks and costs involved. For example, if in order to increase the security of the person with dementia, they need to be constantly monitored for bathing, eating, dressing, etc., up to the point that they feel observed and without the right for privacy, there is probably a higher costs to that person's rights (in terms or privacy, intimacy and autonomy) for what it is obtained in exchange.
- **Non-maleficence**: It means avoiding the causation of harm; if this is not possible, the harm should not be disproportionate to the benefit of the treatment. This can be applied to any medical treatment that may have side effects, but whose main therapeutic goals mean a benefit that overcomes significantly the existence of costs. In the area of ICT, thinking of a robot within an older person's home, the risk of the robot harming the person (hitting them, overriding them, etc.) must be "0". In the IWARD project (www.iward.eu), it was technically established and implemented that the robots developed in the project (which performed orientation, delivery, surveillance and cleaning tasks) needed to keep an approximate distance of 50 cm from any object that may suddenly appear in their way and which could be identifiable as a person, in order to avoid accidental crashes. On a first prototype stage, this required a proper technological definition of which "objects" could be identified as "people" in order to avoid both false positives and false negatives.
- **Autonomy**: On Rivera-Mindt words (2012), it is the "assumption that patient can decide what treatments he/she wants". Thus, the views of the participant's about a particular treatment or intervention need to be respected. According to the Self-Determination Theory explained by Ryan and LaGuardia (2000), there are three basic needs in the human being: autonomy, competence and connectivity. This theory is proposed as a plausible explanation of both social interactions and activities performed while ageing. Autonomy is experienced each time a person perceives his/her behaviour as congruent and self-initiated. Competence refers (within this theory) as the feeling of efficacy with regards to the interactions with social environment and to experimenting opportunities to exercise and express one's own capabilities. Finally, connectivity refers to a feeling of connection and

belonging to significant others. According to the theory, when any of these three psychological needs is frustrated, individuals will show a motivational decline that will derive in a decline of vitality, willingness, integration and wellbeing; moreover, individuals will seek activities, people and relationships by means of which these psychological needs are fulfilled. With regards to older people's autonomy, Ryan and LaGuardia (2000) consider essential that the older people are involved to the maximum extent that is possible with the decision making processes related to changes that have to be done in their environment, in order to preserve their sense of perceived and real control over the events happening in their lives. In order to guarantee this, a key issue will be to provide support to them without communicating messages that make the older person feel useless or a burden for their environment, and without limiting their decision making abilities beyond the limits imposed by an eventual neurodegenerative disorder (like, for example, Alzheimer disease).

- **Transparency**: Goals and purpose for data collection purposes need to be clearly explained to users and families. This relates directly to **informed consent**. According to Berg et al. (2001), the primary purposes of the consent form are (1) to promote individual autonomy, (2) to encourage rational decision-making, and (3) to protect patients' safety and wellbeing. This means that people should know what they are signing up for and if there is any doubt about the person's wish to continue their participation, they should be queried again to guarantee that the person, despite the eventual cognitive problems, is still informed and willing to participate. According to Fisher (2012), the informed consent form must comprise three elements:

  – Appropriate disclosure: users must be given sufficient information and time to make a reasoned choice, according to a document adapted to their language level.
  – A competent participant: a user that is rational and able to understand and appreciate the information presented.
  – Consent voluntarily given: this means that there is no penalty for declining or withdrawing.

  With regards to ethical principles outside Europe, the requirements of the American Psychological Association (2010), present a clear description on the use of informed consent for research. More specifically, when obtaining informed consent as required in Standard 3.10, professionals (psychologists in this particular case, but can be extensive to any situation including patients) must inform participants about:

  – The purpose of the research, expected duration and procedures;
  – The right to decline to participate and to withdraw from the research once participation has begun;
  – The foreseeable consequences of declining or withdrawing;
  – Reasonably foreseeable factors that may be expected to influence their willingness to participate such as potential risks, discomfort, or adverse effects;

  - any prospective research benefits;
  - limits of confidentiality;
  - incentives for participation;
  - whom to contact for questions about the research and research participants' rights.

- **Human integrity**: This principle means that one's physical and psychological conditions should be respected and no one has the right to infringe them without explicit and informed permission. In this regards, one of the most interesting topics studied in the latest years is the "subjective age" or "perceived age". As described by Uotinen, Rantanen and Suutama (2005), numerous studies suggest that people perceiving themselves having actually a lower or younger age that what indicates their ID (i.e. chronological age) are healthier, are more engaged with life and assess their physical and mental status in a more favourable way than those who perceive themselves as belonging to a higher age group than the one they actually belong to. These authors, in a prospective study with a sample of 1,165 subjects and a follow up of 13 years (running from 1988 to 2001) found that those people perceiving themselves as "older" end up suffering from more diseases, have a worst self-reported health status, a worse cognitive status, and a higher score in depression scales when compared with those perceiving themselves as "younger". In which sense this study applies to ICT development and ethics? The answer is that ICTs need to be respectful with the biopsychosocial health conditions of older people, not assuming that they are more deteriorated than they actually are, since increasing the likelihood for older people to see themselves as more "needed-from-support" may lead to undesirable stereotyping of age, more depression, less control over the environment, and, in summary, to the confluence of factors increasing risk of decline and mortality.

Based on the consideration of principles described above, the following section will try to go deeply into some particular considerations that specifically apply to ICT research with older people who age with an underlying process of dementia.

7.3 Special Considerations When Developing ICTs for Older People with Dementia: Preservation of Autonomy, Environmental Control and Balance Between Patients' and Caregivers' Rights

The decline of cognitive functions (especially memory and executive functions – decision taking, abstract reasoning, problem solving, planning, inhibition, judgement –) is probably the most reliable symptom of an underlying neurodegenerative process (American Psychiatric Association 2000). In this scenario, the role of ICTs can be preventive from or, on the contrary, be a promoter of decline. According to Van Hoof et al. (2007), a simple guideline list for developing ICTs for people with

dementia should include: (1) ICTs which do not require any learning; (2) look familiar; (3) do not remove control from the user; and (4) keep user interaction to a minimum. Below, we intend to be more concrete on these issues.

First of all, ICTs should focus on providing a support to maintain autonomy and decision taking as long as possible, empowering the older person as long as the dementia process allows it, instead of being an external cognitive aid that substitutes the person's natural practice of cognition. For example, in the previously mentioned EC funded HERMES project (http://www.fp7-hermes.eu) a memory support system for elderly people with normal cognitive aging and age-related memory decline was developed. Besides support, the goal was to reduce the progression of cognitive decline, thereby reducing the need for active care and support and substantially increasing the ability to cope with everyday life and to live independently. The person was offered to play a game with memory cues in order to recover a specific event of their episodic (i.e. a past visit to the doctor) or prospective (i.e. a future date with your daughter) memory. In order to achieve that, a "life capturing" technology was developed to support episodic memory. Through an ambient intelligence technology events that happen in the user's home were captured by recording audio and video, which was consecutively processed and enriched with contextual metadata to allow retrieving this data based on associative queries for when and where something has happened, what had happened and who was involved. For support of prospective memory, multiple calendaring applications involving advanced activity reminding based on time, location, and person were developed. In terms of autonomy being put in risk, this did not happen, since the device did not provide the whole information to the person; instead, they had to derive it from the clues offered by the HERMES game. In this case, we can talk about a support for cognition.

On the contrary, in FP6 EC funded VITAL project (http://ist.vital.org), one of the worst rated features of the platform developed in the project (Díaz, Garcia, and De Felipe 2010) was a mobile phone event reminder (i.e. it was a mere reminder of appointments that prevented the person to exercise their episodic memory and made them rely on the device, so the person did not need to exercise their memory anymore). Some of the users participated in those two projects' focus groups, and while they liked the first device, they said they wanted to have their own control in terms of setting the reminders by themselves. The mobile phone also offered them a real-time tourist audio guide service, which consisted on popping up information when reaching places of cultural or tourist interest. With regards to this, older users stated that they did not want the device to be configured by somebody else; instead, they wanted to perform an active search on locations and claimed to be independent enough to plan their holidays and trips in advance, with enough personal resources that put them in the position of not needing a device like this at all. On a more positive sense, this project allowed our research team to develop a series of procedures for data protection in ICT related projects (Díaz et al. 2009).

This leads us to the concept of autonomy, and how ICTs should focus on enhancing older people's autonomy, rather than on substituting it or assuming that the person has already lost it. Autonomy can be defined as the ability and exercise of taking one's own decisions in whatever affects daily live (Rivera-Mindt 2012).

Dementia has an impact on older people's live autonomy and any inclusion of technology in these population's lives should ensure the preservation of their autonomy as long as it is possible, being a support rather than a task-maker or performance-substitute that may constraint and reduce the repertoire of behaviours that the old person with dementia is still able (and willing) to do by themselves.

In order to understand the implications of the need to preserve autonomy, probably the environmental control is a concept that needs to be addressed at this point. The person's sense of having control over the environment where they live (over decisions implying their home, the decoration of their room in their nursing home, caring for a pet or a plant, raising vegetables on a small piece of land, etc.) has been defined in literature as a key variable for longevity (if preserved) or as a mortality predictor (if eliminated). Many studies explain how older people who preserve control over their environment and the way it is configured, ordered and built (Colcombe and Kramer 2003; Miller and Lachman 2000; Seeman et al. 2001) show a higher preservation of their cognitive abilities, mood and longevity. Control beliefs involve the perception that one can influence what happens in one's life and to what extent one's actions can bring about desired outcomes such as good cognitive functioning. It includes beliefs or expectations about one's abilities and perceptions about external constraints. As precisely described by Agrigoroaei and Lachman (2011), a lowered sense of control may have affective, behavioural, motivational, and physiological effects, including greater levels of stress and anxiety, lower levels of effort, persistence, and strategy use, as well as less frequent engagement in memory tasks which can impact cognitive performance.

Technologies supporting older people with dementia at their homes should help them keep track of the tasks they are doing, as long as the elderly are still able and willing to do these tasks by themselves. If ICTs intend to deal with this particular set of tasks, they should provide the minimum support that is necessary for the person to keep control of their daily environment (both in terms of basic and instrumental activities of daily living), since a reduction of environmental control may accelerate decline, reduce autonomy and eventually fasten mortality, though the findings about loss of perceived control as a mortality predictor among the older people are still controversial since many years ago (Eizenman et al. 1997).

Furthermore, as long as the person with a cognitive decline, diagnosed or not, is still competent (understood as a preservation to develop coherent decision taking processes that affect themselves or others), they keep responsible for deciding on any issue affecting their daily live activities and their domains. The problem comes when defining competence, since multiple terms with overlapping meanings have risen over the years: "ability", "capacity", etc. (Rivera-Mindt 2012). The primary distinction is legal, and law presumes all adults are competent to make treatment decisions (in other words, incompetence must be proven). However, as Rivera-Mindt (2012) states, competence is routinely questioned in many circumstances, and it needs to be considered that it is "context-dependent", meaning that impaired decision making in one area does not necessarily invalidate capacity in others. According to Marson et al. (1995), mild AD patients may have intact decision-making abilities and no difference in likelihood of assenting from other non-demented subjects.

Also, they appear quite preserved when it comes to express choice, to express that choice reasonably, to appreciate the consequences and to provide rational reasons. Actually, according to Lapid et al. (2004), older people with severe depression may be at a great risk for decision making impairments.

In terms of ICT inclusion, this means that people with dementia need to be consulted and informed properly when trying to introduce new technologies in their daily environment, as the final word in terms of decisions is theirs. Even when conflicts between patients' and their caregivers' opinions and desires may rise, the decisions from the person who is the target user of that technology should be respected when the person is still able to reasonably decide on topics affecting his/her daily life (Enable Project 2004). However, there is a need to properly intervene with the caregivers to avoid feelings of guilt (Thompson and Gallagher-Thompson 1996; Carod-Artal et al. 1999; Garre-Olmo et al. 2002; Devi and Ruiz-Almazán 2002). According to Hughes et al. (2002), caregivers are concerned that, for the sake of safety, liberty of the person with dementia needs to be restricted. In this study, some recommendations were drawn for caregivers when treating with people with dementia, which may also be applied to any person not familiarized in dealing with people with a neurodegenerative disease. Those recommendations include: avoiding infantilization, communication of what it is important, provision an informed consent for any procedure implying the person's participation, avoiding talking about people with dementia in front of them as if they were not there, and, in sum, treating the person as a person (recognition and validation). Next section will report some good practices on how to deal with these recommendations, before final remarks and conclusions are presented.

7.4 Examples of Good Practices in the Past and Final Remarks

One of the main sources on good practices related to ICT and Ethics can be reached on the website called *ICT & Ageing – European Study on Users, Markets and Technologies* (http://www.ict-ageing.eu). Among these, the EnableAge project show how great efforts can and should be deployed in order to give people with dementia themselves the possibility to consent or not, rather than rely on consent by proxy from family carers. According to the document on good ethical practices in EnableAge, informed consent was dealt with in each country in conformance with the 'Helsinki Declaration' (World medical Association's Ethical Principles for Medical Research Involving Human Subjects), with reference to local ethics committees as appropriate. Practically, considerable effort was expended to ensure that consent really was 'informed' and freely given, and not because of feelings of being pressured by a health care professional or their carer. Moreover, consent was renewed on an on-going basis during the trials and participants had an open opportunity to withdraw if they wished. More importantly, as it may be a constant issue in projects involving conflicts between the patients' and caregivers' desires. In such contexts the trial was terminated if the user with cognitive decline or dementia definitely rejected the

product. In one case the carer did not find the product beneficial but the user wished to continue; in that case the trial was continued. In other cases, where the carer was keener than the person cared for, but there was no outright rejection, the trials proceeded on the basis of beneficence for the situation as a whole. What does this particular case tell us regarding the ethical principles that need to be applied to ICT research for people with dementia? It tells us that, putting enough effort, attention and time, open and informed consent can be achieved by researchers, even from users with dementia.

In summary, and driven more from the need of respecting the target users' needs, even if these are suffering from a neurodegenerative disease, it is very likely that technology should probably focus less on security, and probably focus more on the preservation of dignity and autonomy, among other principles, of the people with dementia. The thin line between a safe living environment and a home that maintain the older person's autonomy and dignity is a source of high controversy when it comes to deal with older people for which there are no definitive standards for a competency assessment. In other words, each case has to be studied with all the particularities it may comprise, since the establishment of general rules or guidelines for the ICT involvement of all the people with dementia is a hard task which leads to new questions and dilemmas. We have tried in this chapter to establish some recommendations based on our own practice, but to what extent this may be applicable to all the environments is a question that researcher need to answer, based on (1) their knowledge on ethics and the specific rules applied to the occupation and country where they live, (2) on their experience with older people, and, most importantly, (3) on their common sense. Something not to be forgotten is that technology can be a supplementary solution, but never a substitution of care and face-to-face contact and social support. A robot may never substitute the human touch, but it may help with some particular tasks and goals. Finally, even if obviousness comes to the stage, there is a need to remind the reader that the person with dementia is still a person in their whole integrity and they have the ultimate choice when faced with decision-making about their daily life and environment. Clearly, there is still a lot to learn and share about older people, especially if they have dementia, and still there are many stereotypes about aging to be overcome by professionals of all the research community. We hope this chapter contributes to throw a little light on this issue and provides help in this sense.

References

Agrigoroaei, Stefan, and Margie E. Lachman. 2011. Cognitive functioning in midlife and old age: Combined effects of psychosocial and behavioral factors. *Journal of Gerontology* 66B: il30–il40.

Ajzen, Icek. 1991. The theory of planned behavior. *Organizational Behaviour and Human Decision Processes* 50: 179–211.

American Psychiatric Association. 2000. *Diagnostic and statistical manual of mental disorders (text rev.)*, 4th ed. Washington, D.C.: American Psychiatric Association.

American Psychological Association. 2010. Amendments to the 2002 "Ethical principles of psychologists and code of conduct". *American Psychologist 65*(5): 493.

Berg, Jessica W., Paul S. Appelbaum, Charles W. Lidz, and Lisa S. Parker. 2001. *Informed consent: Legal theory and clinical practice*. New York: Oxford University Press.

Carod-Artal, Francisco J., J.A. Egido-Navarro, J.L. González-Gutierrez, and E. Varela de Seijas. 1999. Perception of long term over burden in caregivers of stroke survivors [article in Spanish]. *Revista de Neurologia* 28: 1130–1138.

Cimperman, Miha. 2010. Telemedicine adoption by Elderly Consumers – A theoretical model. In *Economic and business review (EBR) 1st annual conference*, Ljubljana, Slovenia, 2 Dec 2010.

Colcombe, Stanley J., and Arthur F. Kramer. 2003. Fitness effects on the cognitive function of older adults: A meta-analytic study. *Psychological Science* 14: 125–130.

Consolvo, Sunny, Peter Roessler, and Brett E. Shelton. 2004. The CareNet display: Lessons learned from an in home evaluation of an ambient display. *UbiComp 2004, LNCS 3205*, 1–17.

Coughlin, Joseph F., Lisa A. D'Ambrosio, Bryan Reimer and Michelle R. Pratt. 2007. Older adult perceptions of Smart Home Technologies: Implications for research, policy & market innovations in healthcare. In *Proceedings of the 29th annual international conference of the IEEE EMBS*, Lyon, 23–26 Aug 2007.

Deví, Josep, and Isabel Ruiz-Almázan. 2002. Models of stress and coping in the caregiver of the patient with dementia [article in Spanish]. *Revista Multidisciplinar de Gerontología* 12: 31–37.

Díaz, Unai, Cristina Buiza, Elena Urdaneta, and Jose Javier Yanguas. 2009. Handling of privacy and data protection issues in VITAL Project: A working model for EC funded projects. In *Adjunct proceedings – 3rd Europian conference on ambient intelligence (AmI09). Roots for the future of ambient intelligence*, ed. Manfred Tscheligi, Borys de Ruyter, John Soldatos et al. Salzburg, Austria.

Díaz, Unai, Alvaro Garcia, and Alejandro De Felipe. 2010. A new tourist audio guide service for elderly people integrated in the Mobile Phone: Preliminary results. Paper presented at the *3rd ACM international conference on PErvasive technologies related to assistive environments (PETRA 2010)*, Samos, Greece, 23–25 June 2010.

Diaz, Unai, Alvaro, Garcia, and Elena, Urdaneta. 2010. What elderly users do not want from technology: A qualitative approach. *Gerontechnology* 9(2): 210.

Eizenman, Dara R., John R. Nesselroade, David L. Featherman, and John W. Rowe. 1997. Intraindividual variability in perceived control in an older sample: The MacArthur successful aging studies. *Psychology and Aging* 12: 489–502.

ENABLE Project. 2004. Final Methodology Report. www.enableproject.org.

European Union. 1995. Directive 95/46/EC of the European European Union and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, http://www.cdt.org/privacy/eudirective/EU_Directive_.html.

European Union. 1997. Directive 97/66/EC of 15 December 1997 of the European Parliament and of the council concerning the processing of personal data and the protection of privacy in the telecommunications sector. http://www.unhcr.org/refworld/docid/3ddcc6364.html. Accessed 15 Dec 1997.

Fisher, Celia B. 2012. *Decoding the ethics code: A practical guide for psychologists*. Updated 2nd ed. Thousand Oaks: Sage Publications.

Garre-Olmo, Josep, Secundino López-Pousa, Joan Vilalta-Franch, Antoni Turón-Estrada, et al. 2002. Caregiver's burden and depressive symptoms in patients with Alzheimer's disease. A 12 month follow-up [article in Spanish]. *Revista de Neurologia* 34: 601–607.

HERMES Consortium. 2008. Hermes – Cognitive care and guidance for active aging. EU FP7 Specific Targeted Research Project. http://www.fp7-hermes.eu. Accessed 14 Feb 2012.

Hughes, Julian C., Tony Hope, Steve Reader, and Dee Rice. 2002. Dementia and ethics: The views of informal carers. *Journal of the Royal Society of Medicine* 95: 242–246.

ICT & Ageing – European Study on Users, Markets and Technologies. (http://www.ict-ageing.eu).

Jiang, Jianmin, Arjan Geven, and Shaoyan Zhang. 2008. HERMES: A FP7 funded project towards computer-aided memory management via intelligent computations. Paper presented at the *3rd*

symposium of ubiquitous computing and ambient intelligence 2008, 249–253. New York: Springer. doi: 10.1007/978-3-540-85867-6_29. Accessed 16 Feb 2012.

Lapid, Maria I., Teresa A. Rummans, V. Shane Pankratz, and Paul S. Appelbaum. 2004. Decisional capacity of depressed elderly to consent to electroconvulsive therapy. *Journal of Geriatric Psychiatry and Neurology* 17: 42–46.

Marson, Daniel C., Kellie K. Ingram, Heather A. Cody, and Lindy E. Harrell. 1995. Assessing the competency of Alzheimer's disease patients under different legal standards: A prototype instrument. *Archives of Neurology* 52: 949–954.

Miller, Lisa M.S., and Margie E. Lachman. 2000. Cognitive performance and the role of control beliefs in midlife. *Aging, Neuropsychology and Cognition* 7(2): 69–85.

Pauwels, Eléonore. 2007. *The UK Department of Health's best practice guide – Independence, choice and risk – Good practice for dealing with risk in the domain of social care*. European Commission: Ethics for researchers, Facilitating research excellence in FP7. Brussels: European Commission.

Phang, Chee W., Juliana Sutanto, Atreyi Kankanhalli, Li Yan, Chuanhoo Tan, and Hock Hai Teo. 2006. Senior Citizens' acceptance of information systems: A study in the context of E-government services. *IEEE Transactions on Engineering Management* 53: 555–569.

Rivera-Mindt, Monica. 2012. Ethical decision making and capacity to consent in neurocognitively impaired and vulnerable patient populations. Paper presented at the *40th meeting of the International Neuropsychological Society*, Montreal, 18 Feb 2012.

Royal Decree 223/2004, 6th February, by means of which clinical trials with medications are regulated, BOE, 33. 7 Feb 2004, 5429–5443.

Ryan, Richard M., and Jennifer G. La Guardia. 2000. What is being optimized?: Self-determination theory and basic psychological needs. In *Psychology and the aging revolution. How we adapt to longer life*, ed. Sara H. Qualls and Norman Abeles, 145–172. Washington, DC: American Psychological Association.

Seeman, Teresa E., Tina M. Lusignolo, Marilyn Albert, and Lisa Berkman. 2001. Social relationships, social support, and patterns of cognitive aging in healthy, high-functioning older adults: MacArthur studies of successful aging. *Health Psychology* 20: 243–255.

Spanish Organic Law, 15/1999, for protection of data of personal nature, BOE, 298, 14 Dec 1999, 43088–43099.

Thompson, Larry W., and Dolores Gallagher-Thompson. 1996. Practical issues related to maintenance of mental health and positive well-being in family caregivers. In *The practical handbook of clinical gerontology*, ed. Laura L. Carstensen, Barry A. Edelstein, and Laurie Dornbrand, 129–150. London: Sage.

United Nations. 1948 The Universal Declaration of Human Rights (online). Accessed 1 Apr 2012. http://www.un.org/en/documents/udhr/.

Uotinen, Virpi, Taina Rantanen, and Timo Suutama. 2005. Perceived age as a predictor of old age mortality: A 13-year prospective study. *Age and Ageing* 34: 368–372.

Van Hoof, Joost, H.S.M. Kort, P. Markopoulos, and M. Soede. 2007. Ambient intelligence, ethics and privacy. *Gerontechnology* 6: 155–163.

van Veldhoven, Erwin R., Martin H. Vastenburg, and David V. Keyson. 2008. Designing an interactive messaging and reminder. In *Proceedings of AmI 2008*, Nuremberg, 19–22 Nov 2008, 126–140.

Part III
Privacy by Design

Chapter 8
Privacy by Design: Leadership, Methods, and Results

Ann Cavoukian

8.1 Introduction

In October 2010, a landmark resolution was unanimously approved by International Privacy Commissioners and Data Protection Authorities at their annual conference, recognizing *Privacy by Design* (*PbD*) as an "essential component of fundamental privacy protection." The Resolution, which was co-sponsored by Commissioners from Canada, Berlin, New Zealand, the Czech Republic, and Estonia, also:

"Encourages the adoption of the principles of *Privacy by Design* as part of an organization's default mode of operation; and invites Data Protection and Privacy Commissioners to promote *Privacy by Design*, foster the incorporation of its Foundational Principles in privacy policy and legislation in their respective jurisdictions, and encourage research into *Privacy by Design*."[1]

Since then, the *Privacy by Design* Principles have been translated into 25 languages, and public policymakers in the United States and Europe have issued proposals and recommendations for them to be expressed in reformed governance and oversight regimes for managing personal information by organizations.[2] More than a concept, *Privacy by Design* is becoming a legal and regulatory requirement in major jurisdictions around the world.

[1] International Conference of Data Protection and Privacy Commissioners (2010). Privacy by Design Resolution, adopted at Jerusalem, Israel, October 27–29, 2010.

[2] See "EU Commission proposes a comprehensive reform of the data protection rules" (January 25, 2012) at http://ec.europa.eu/justice/newsroom/data-protection/news/120125_en.htm and "FTC Issues Final Commission Report on Protecting Consumer Privacy", Press Release, 26 March 2012 at www.ftc.gov/opa/2012/03/privacyframework.shtm

A. Cavoukian, Ph.D. (✉)
Information and Privacy Commissioner, 2 Bloor Street East, 14th Floor,
Toronto, ON, Canada, M4W 1A8
e-mail: Commissioner@ipc.on.ca; fred.carter@ipc.on.ca; michelle.chibba@ipc.on.ca

S. Gutwirth et al. (eds.), *European Data Protection: Coming of Age*,
DOI 10.1007/978-94-007-5170-5_8,

This paper explains how *Privacy by Design* Foundational Principles build upon universal Fair Information Practice Principles (FIPPs) in a way that updates and adapts them to modern information management needs and requirements. By emphasizing proactive leadership and goal-setting, systematic and verifiable implementation methods, and demonstrable positive-sum results, *Privacy by Design* principles can assure effective organizational data protection and privacy in the Information Age by:

- reducing harms and other "unintended" consequences associatedwith personal information;
- promoting market-based innovation and competitiveness;
- demonstrating effectiveness and credibility of data management practices;
- serving as a framework for domain-specific control objectives and best practices;
- earning the confidence and trust of clients, partners, and the public;
- strengthening internal accountability mechanisms; and
- supporting regulatory and third-party oversight efforts.

Privacy by Design Foundational Principles serve as an overarching framework for privacy and data protection early, effectively, and credibly into information technologies, organizational processes, networked architectures and, indeed, entire systems of governance and oversight.

This essay offers a short contextual history and overview of the *Privacy by Design* concept, contrasting it with existing fair information principle approaches, and pointing out future challenges.

8.2 Evolving Privacy Contexts

Privacy and data protection[3] are often said to be in "crisis" today as a consequence of many trends and factors, including:

- leapfrogging information and communications technology developments;
- the advent of social, cloud, mobile, and ambient computing;
- evolving cultural norms; and
- a global patchwork of outdated privacy laws.

[3] I acknowledge that the terms "privacy" and "data protection" refer to differing but closely related concepts. I recognize that privacy is a much broader concept than data protection, with the latter term typically referring to an individual's information rights, along with the legal structures that enable them and impose obligations on organizations that process personal data. *Privacy by Design* principles seek the highest possible global standard of privacy, but are agnostic with respect to specific legal privacy rights and obligations that may exist in any given jurisdiction. For some thoughtful discussions about privacy and data protection, and the distinctions between them, see Viktor Mayer-Schönberger (1997), Omer Tene (2010), Colette Cuijpers (2007), and András Jóri (2007).

The advent of networked information and communications technologies has, in one generation, radically changed the rules for managing data. Current trends carry profound implications for privacy. The global creation of data is accelerating, and is everywhere being replicated and stored, resulting in "oceans of data." We can no longer speak meaningfully of information destruction, as we once did with paper records, because digital bits and bytes have now attained near immortality in cyberspace, thwarting efforts to successfully remove them from "public" domains. The practical obscurity of personal information – the default privacy and data protection of yesteryear – is disappearing as data becomes digitized, connected to the grid, and exploited in countless new ways. We've all but given up trying to inventory and classify information, and now rely more on advanced searching techniques and automated tools to manage and "mine" it. The combined effect is that while information has become cheap to distribute, copy, and recombine – too cheap to meter – personal information has also become far more available and consequential, and at the same time far more difficult to control and protect.

The information privacy solution requires a combination of data minimization techniques, credible safeguards, individual participation in data processing lifecycles, and robust accountability measures by data processors who are informed by an enhanced and enforceable set of universal privacy principles better suited to modern realities.

If personal data is the currency of the modern global economy, then *trust* is the Central Bank. Misuses and abuses of personal data erode informational self-determination, cause harms, and corrode the confidence and trust needed for innovative economic growth and prosperity.

8.3 Origins and Evolution of *Privacy by Design*

Privacy by Design evolved from early efforts to express Fair Information Practice principles directly in the design and operation of information and communications technologies, resulting in *Privacy Enhancing Technologies* (PETs). Over time, the broader systems and processes in which PETs were embedded and operated were also considered.[4]

[4] For an extended treatment of *PbD* origins, see Ann Cavoukian (2012), "*Privacy by Design*: Origins, Meaning, and Prospects for Assuring Privacy and Trust in the Information Era," in *Privacy Protection Measures and Technologies in Business Organizations: Aspects and Standards*, ed. George O.M. Yee, 178–208 (Ottawa, Canada: Aptus Research Solutions Inc. and Carleton University).

8.3.1 The Shift to Positive-Sum (Not Zero-Sum) Thinking

The events and consequences of September 11 challenged assumptions among many public policy makers, privacy advocates, freedom fighters, and technologists, that individual privacy was necessarily paramount to other interests in society. Historically, privacy has been a socio-culturally determined value, waxing and waning in response to various determinants, but privacy advocates found it increasingly difficult to defend privacy interests in an atmosphere characterized by visceral public fears, desires for collective security, and the right "not to be blown to pieces."

Almost overnight, the privacy threat models changed. Public authorities enacted security legislation and put in place initiatives that trumped information privacy rights, enlisting public- and private-sector organizations to collect, use, and disclose more (and more granular) personal data for secondary purposes, such as public safety. At the same time, information networks were becoming more complex and sophisticated, undermining the dominant "client-server" transaction model by removing data subjects from the client side of the equation entirely. How could privacy be assured when the collection, disclosure, and use of personal information might not even involve the individual at all?[5]

A zero-sum paradigm prevailed: more of one good (e.g., public security, fraud detection, operational control) would require less of another good (individual privacy, freedom). But this win/lose mentality, sometimes enlisting the "balance" metaphor, posed a threat to privacy, given the public appetite for safety was very high.

My Office challenged the premise that privacy and data protection necessarily had to be ceded in order to gain public, personal, or information security benefits, arguing that multiple goals could be achieved concurrently. Many security technologies and information systems could be designed (or redesigned) to be effective while minimizing or even eliminating their privacy-invasive features.[6]

The proper paradigm was *positive*-sum, not zero-sum. My Office challenged the privacy community, specification writers, and solution providers to raise the level of debate on security and privacy above simplistic, either/or viewpoints; to set appropriate procurement specifications; and to embed privacy and data protection principles into the concept, design, and implementation of all technology-enabled solutions.[7]

The broadening context for evaluating privacy risks and applying data protection principles went well beyond a narrow fixation on information communication technologies (ICTs) to include the "soft" legal, policy, procedural, and other organizational controls and operating contexts in which PETs might be embedded.

---

[5] For a discussion, see Ann Cavoukian, *Privacy in the Clouds*, 2008a.

[6] See Ann Cavoukian, *Transformative Technologies Deliver Both Security and Privacy: Think Positive-Sum not Zero-Sum*, 2009b. (Accessed at: www.ipc.on.ca/images/Resources/trans-tech.pdf), and *Moving Forward from PETs to PETs Plus: The Time for Change is Now*, 2009a (Accessed at: www.ipc.on.ca/images/Resources/petsplus_3.pdf).

[7] Ann Cavoukian (2002).

A holistic, integrative approach to assuring privacy required taking into account developments in other areas, including:

- **Evolving legal and regulatory requirements**: Legal, regulatory, and contractual requirements that apply to an organization's processing of personally identifiable information (PII) are starting points for designing, operating, and evaluating information management systems in a holistic, accountable manner. But data privacy, security, accountability, and law enforcement requirements were multiplying across sectors and jurisdictions during the first decade of the millennium – challenging straightforward data protection compliance requirements.[8]
- **Evolving organizations**: Firms were undergoing profound changes in response to evolving business environments, and their information management needs were changing along with their business models and operational structures. In response to market imperatives, organizations were becoming technology- and data-intensive, decentralized, service-oriented, hierarchically-flat, flexible, innovative – and global. Managing a database would never be the same again.[9]
- **Evolving computing and networked contexts**: Ongoing revolutions in processing power, data storage, sensors, and communication networks were fuelling rapid innovation. Personal data became more voluminous and more granular – and more ubiquitous, semi-public, and instantly retrievable at the same time. Mirroring the Internet itself, networks of all kinds were becoming more complex, sophisticated, and decentralized. The emergence of cloud, mobile, and social computing platforms was altering traditional information flows in dramatic new ways, posing daunting challenges for data protection.
- **Evolving consumer expectations and tastes**: Complicating matters further, it was becoming evident that individuals and consumers weren't always opposed to new "privacy-invasive" innovations and services. While they wanted privacy and control, they also wanted the many conveniences, efficiencies, and benefits of "free" services in exchange for their personal information. Consumers didn't always understand, or want, complete and granular control over their personal information, opting instead to trust the reputations and the behaviour of personal data custodians.

In these contexts, the faith in privacy-enhancing technologies or "code" alone to ensure privacy and data protection seemed, at best, naïve. The failure of most consumer-facing privacy-enhancing tools and services to attract sufficient market success only reinforced the understanding that a more holistic and more robust approach to protecting and promoting privacy was necessary.[10]

[8] Colin Bennett (2009).

[9] Tapscott and Cavoukian (2006).

[10] See Simone Fischer-Hübner et al., Online Privacy: Towards Informational Self-Determination on the Internet ("Dagstuhl Manifesto"), 2011.

8.3.2 Emphasis on Practical Results and Outcomes

Privacy remains a human right in many quarters, but abstract principles and rights-based arguments for data protection rules have not had an easy time winning the day against many "competing" interests.[11] It was becoming less clear how privacy rights should be given effective expression, especially in a fast-changing global environment.

A more preventative, practical, evidence-based approach was becoming necessary in the first decade of the millennium. This meant encouraging clear promises to be made and kept. It meant emphasizing practical, measurable, and immediate results, based on universally-agreed-upon privacy values, common frameworks for integrating the diverse interests at play in exploiting personal information, and benchmarks for assessing adherence.

Fair Information Practice Principles have served as universal privacy values and as a common general framework for translating privacy and data protection objectives to law, policy, and technologies. Many variants of FIPPs exist and are in force around the world today, varying in length, detail, and force of application. Despite superficial differences, they all share common fundamentals. At the broadest conceptual level, all privacy and data protection principles seek both *opacity* and *transparency* of data processing. Opacity-enhancing principles seek to *restrict* unauthorized data processing by minimizing and safeguarding data, while transparency-enhancing principles seek to *enhance* visibility and accountability by involving data subjects in the data processing lifecycle, and by establishing governance requirements for data processors. All FIPPs express four "meta-FIPPs:" Data Minimization, Safeguards, User Participation, and Accountability (see Table 8.1).

The enduring confidence of individuals, businesses, and regulators in organizations' data-handling practices is a function of their ability to express the FIPPs' core requirements, which also promote efficiencies, innovation, and competitive advantages. Privacy *is* good for business.

Privacy by Design Foundational Principles build upon established FIPPs, and seek to raise the bar for privacy and data protection by promoting enhanced accountability and trust through:

1. proactive leadership and goal-setting;
2. systematic and verifiable implementation methods; and
3. practical and demonstrable outcomes.

These new *process* design principles are expressed by three of *PbD*'s Foundational Principles: *Proactive not Reactive; Embedded into Design;* and *Full Functionality – Positive-Sum, not Zero-Sum*, as the table below summarizes. The four other *Privacy by Design* Principles map well to existing Fair Information Practice principles and, hence, to current methods already in place for interpreting, applying, and verifying data protection controls.

[11] See Privacy International et al. (1998, 2003, 2007, 2011), Ford (2004).

Table 8.1 Fair information practices and *Privacy by Design* principles

FIPPS	Meta-FIPPS	*Privacy by Design*
Purpose specification	Data minimization	Privacy as the default (setting)
Collection limitation		
Use, retention and disclosure limitation		
Safeguards	Safeguards	End-to-end security
Informed consent	User participation	Respect for user privacy
Accuracy		
Access		
Redress		
Accountability (to data subject)		
Accountability	Accountability (other than data subject)	Openness and transparency
Openness		
Compliance		
	Leadership and goal-setting	Proactive not reactive; Preventative not remedial
	Systematic and verifiable methods	Privacy embedded into design
	Practical and demonstrable results	Full functionality – positive-sum, not zero-sum

8.4 *Privacy by Design* Foundational Principles

8.4.1 Opacity-Enhancing Principles

Opacity-enhancing principles seek to prevent or restrict data processing to a minimum. Data that is not collected or retained, or which is secured and unavailable, cannot be misused or abused. Strong safeguards and data minimization practices are opacity-enhancing. The advent of mandatory data breach disclosure and notification requirements provides strong incentives for organizations to apply opacity principles with vigour.

8.4.1.1 Privacy as the Default Setting (Data Minimization)

Data that is not collected, retained, or disclosed is data that does not need to be protected, managed, or accounted for. Data that does not exist cannot be accessed, altered, copied, enriched, shared, lost, hacked, or otherwise used for secondary and unauthorized purposes. This *PbD* Principle is premised on the idea that the starting point for designing information technologies and systems should always be maximally privacy-enhancing. The default configuration or settings of technologies, tools, platforms, or services offered to individuals should be as restrictive as possible

regarding use of personally identifiable data. The *Privacy as the Default* Principle is informed by the following FIPPs:

- **Purpose Specification**: The purposes for which personal information is collected, used, retained, and disclosed should be communicated to the individual (data subject) at or before the time the information is collected. Specified purposes should be clear, limited, and relevant to the circumstances.
- **Collection Limitation**: The collection of personal information must be fair, lawful, and limited to that which is necessary for the specified purposes.
- **Data Minimization**: The collection of personal information should be kept to a strict minimum. The design of information and communications technologies, organizational processes, and networked infrastructures and systems should begin with non-identifiable interactions and transactions as the default. Wherever possible, the identifiability, observability, and linkability of personal information should be minimized.
- **Use, Retention, and Disclosure Limitation**: The use, retention, and disclosure of personal information should be limited to the relevant purposes identified to the individual, for which he or she has consented with full knowledge (except where otherwise required by law). Personal information should be retained only as long as necessary to fulfill the stated purposes, and then securely destroyed.

Where the need for personal information is not clear, there should be a presumption of privacy and the precautionary principle should apply: the default settings should be the most privacy protective.

The *Privacy as the Default* Principle expresses the concept of always starting with the minimum personal data possible and then justifying additional collection, disclosure, retention, and use on an exceptional and specific data-by-data basis.

8.4.1.2 End-to-End Security (Safeguards)

This *Privacy by Design* Principle embraces data security methods and goes further to emphasize the need for safeguards to be applied in a comprehensive and systematic manner. Confidentiality, integrity, and availability of data should be continuously assured across the entire domain and throughout the lifecycle of the data in question. There should be no gaps in protection or oversight. The *Safeguards* Principle has special relevance because, at its essence, without strong data security, there can be no privacy.

- **Security**: Organizations are responsible for the security of personal information (generally commensurate with the degree of sensitivity) in their custody and care throughout its entire lifecycle, consistent with criteria and methods developed by recognized standards development bodies.
- **Applied Security Standards** should assure the confidentiality, integrity, and availability of personal data throughout its lifecycle including, *inter alia*, strong

access controls, effective logging and auditing functions, appropriate encryption, and methods of secure destruction.
- **End-Point Devices, User Tools, and Interfaces** should be designed with maximum data security in mind, taking into account identified risks such as loss, theft, tampering, and human error.

Information security is like a chain – it is only as strong as its weakest link. Assuring end-to-end security requires a systematic and iterative approach to be truly credible and effective.

8.4.2 Transparency-Enhancing Principles

In contrast to opacity-enhancing principles, transparency-enhancing principles seek to make the data processing that does occur more visible and subject to scrutiny and verification. Transparency can be preventative when it increases the likelihood of detecting abuses, deterring the adoption of substandard policies and behaviours, and heightening accountability in general.

8.4.2.1 Respect for User Privacy (User Participation)

Information self-determination refers to the right or ability of individuals to exercise a measure of control over their personal data, and serves as the foundation of modern information privacy. The most privacy-enhancing solutions and results are usually those that are consciously designed around the interests, needs, and expectations of individuals and users, who typically have the greatest vested interest in the management of their personal data by others.

Empowering data subjects to play active roles in the management of their own personal data may be the single most effective check against abuses and misuses by others. *Respect for User Privacy* remains at the heart of *PbD* Principles since the early days of PETs, and is supported by the following FIPPs:

- **Consent**: The individual's informed, free, and specific consent should be required for the collection, use, or disclosure of personal information, except where not required by law. The greater the sensitivity of the data, the clearer and more specific the quality of the consent required. Consent may be withdrawn by the individual at a later date.
- **Access**: Individuals should be provided access to their personal information and informed, in a convenient, understandable, and secure manner, of its uses and disclosures.
- **Accuracy**: Personal information should be as accurate, complete, and up to date as is necessary to fulfill the specific purposes. Individuals should be able to

challenge the accuracy and completeness of the information and have it amended as appropriate.
- **Compliance**: Organizations should establish complaint and redress mechanisms, and communicate information about them to data subjects, including how to access the next level of appeal.

Respect for User Privacy goes beyond these FIPPs, and extends to the need for interfaces to be human-centered, user-centric, and user-friendly, so that informed privacy decisions may be reliably made. Similarly, organizational policies and processes and physical architectures should also demonstrate the same degree of consideration for the individual.

There is much variation around the world in how these "user-centric" FIPPs have been interpreted and applied in various contexts. Notwithstanding these variations, it is vitally important to seek, whenever designing information technologies and systems, where and how best to involve individuals at critical points in the personal data lifecycle.

8.4.2.2 Visibility and Transparency (Accountability)

As noted above, visibility and transparency are essential to establishing accountability and trust – not just for individual data subjects in order to ensure informed decisions and the exercise of privacy rights, but, increasingly, for business partners, regulators, and shareholders. This *PbD* Principle tracks well to Fair Information Practices in their entirety, but for assessment and auditing purposes, special emphasis may be placed upon the following FIPPs:

- **Accountability**: The collection of personal information entails a duty of care for its proper management and protection. Responsibility for privacy-related policies and procedures should be documented, communicated to stakeholders and interested parties, and assigned to a specified individual. When transferring personal information to third parties, equivalent data protections through contractual and other means should be secured.
- **Openness**: Openness and transparency are key to accountability. Information about the policies and practices relating to the management of personal information and data protection should be made readily available not only to individuals, but to business partners, regulators, shareholders, and other interested parties.
- **Compliance**: Complaint and redress mechanisms should be established, and information communicated about them, including how to access the next level of appeal, to individuals. Necessary steps to monitor, evaluate, and verify compliance with privacy policies and procedures should be taken and, where appropriate, the results shared with oversight authorities, business partners, and other stakeholders.

In today's hyper-networked world, the trustworthiness, reputation, brand, and success of a technology, organization, or system is increasingly reliant on the behaviour and actions of external forces and actors. With greater scrutiny being applied to

information-handling practices by business outsourcers and regulators alike, visibility and transparency of data protection operations is essential to success.

8.4.3 Process Principles

Thus far, we have described four "meta-FIPPs" and shown how they correlate to four fundamental *Privacy by Design* Principles.

Now we turn to three "new" principles that speak to the method of interpreting and applying the Fair Information Practice Principles in a robust, systematic, and verifiable way. The *Privacy by Design* Principles of *Proactive Not Reactive, Preventative Not Remedial*; *Privacy Embedded into Design*; and *Full Functionality – Positive-Sum not Zero-Sum* extend the FIPPs in the most robust manner possible to meet the privacy and data protection challenges and requirements of the twenty-first century.

8.4.3.1 Proactive Not Reactive; Preventative Not Remedial (Leadership & Goal-Setting)

Privacy by Design Principles aspire to the highest global standards of practical privacy and data protection possible, to go beyond compliance and achieve visible evidence and recognition of leadership, regardless of jurisdiction. Good privacy doesn't just happen by itself – it requires proactive and continuous goal-setting at the earliest stages.

Whether applied to information technologies, organizational practices, physical designs, or networked information ecosystems, global leadership in data protection begins with explicit recognition of the benefits and value of adopting strong privacy practices, early and consistently (e.g., preventing data breaches from occurring). This implies:

- A clear commitment, at the highest levels, to prescribe and enforce high standards of privacy and data protection – generally higher than the standards set out by global laws and regulation.
- A demonstrable privacy and data protection commitment that is shared by organization members, user communities, and stakeholders, in a culture of continuous improvement.
- Establishing methods to recognize poor privacy and data protection designs, to anticipate poor practices and outcomes, and to correct any unintended or negative impacts, well before they occur, in proactive, systematic, and innovative ways.
- Continuous commitment and iterative processes to identify and mitigate privacy and data protection risks.

The preventative and systematic approach to engineering privacy and data protection is often associated with privacy-enhancing technologies. As noted above, a focus on specific information and communications technologies remains a source

of inspiration for building in privacy and data protection principles from the outset. This has been especially true of new and emerging information technologies with privacy-invasive implications such as, for example, video surveillance, biometrics, radio-frequency identification (RFID), electronic road toll systems, "smart" meters, federated identity systems, and whole body imaging scanners, among others.

While *Privacy by Design* concepts are often best illustrated by specific technologies (the more user-centric the better), it is the *organization* that has become a more central and effective focus for applying *PbD* Principles, especially in view of the requirement to comply with privacy and data protection laws. The case for strong organizational privacy and data protection focuses, in essence, on gaining and keeping client trust, loyalty, repeat and higher-value business, and avoiding costly "churn." The value proposition typically breaks down as follows:

1. Client trust drives successful customer relations management and lifetime value – in other words, revenues;
2. Broken trust will result in a loss of market share, loss of revenue, and lower share value;
3. Client trust hinges critically on the strength and credibility of an organization's privacy policies and data protection practices.

The "privacy payoff" also works in reverse: that is, poor privacy leadership, policies, or data protection practices result in additional costs and foregone opportunities and revenues. A lack of attention to data protection could have many negative consequences, including:

- harm to clients or customers whose personal data is used or disclosed inappropriately;
- damage to an organization's reputation and brand;
- financial losses associated with deterioration in the quality or integrity of personal data;
- financial losses due to a loss of business or delay in the implementation of a new product or service due to privacy concerns;
- loss of market share or a drop in share price following negative publicity;
- violations of privacy and data protection laws; and
- diminished confidence and trust in the industry as a whole.[12]

Being proactive and preventative requires a clear understanding of the strategic risks, challenges, and rewards of applying strong data protection throughout an organization and across information systems in a thorough manner.

8.4.3.2 Privacy Embedded into Design (Systematic & Verifiable Methods)

Information and communications technologies, systems, and networks have become extraordinarily complex. Data processing is increasingly interdependent and opaque

[12] See Ponemon 2010–2011.

in nature, defying easy understanding, requiring more trust than ever from stakeholders and users to be sustainable. These are not ideal conditions for ensuring that accountability, data protection, and individual privacy will thrive.

Privacy commitments and data protection controls must be embedded into technologies, operations, and information architectures in a holistic, integrative, and creative way:

- Holistic, because additional, broader contexts should always be considered for a proper assessment of privacy risks and remedies.
- Integrative, because all stakeholders and interests should be consulted and become part of the development dialogue.
- Creative, because embedding privacy rights and data protection controls sometimes means re-inventing existing choices because existing alternatives are unacceptable.

A systematic, principled approach to embedding privacy and data protections should be adopted – one that relies upon accepted standards and process frameworks, and which are amenable to external reviews and audits. All fair information practices should be applied with equal rigour, at every step in design and operation.

Wherever possible, detailed privacy impact and risk assessments should be carried out and published, clearly documenting the privacy and data protection risks and all measures taken to mitigate those risks, including consideration of alternatives and the selection of metrics.

The privacy impacts of the resulting technology, process, or information architecture, and their uses, should be demonstrably minimized, and not easily degraded through use, misconfiguration, or error.

Early efforts to systematically integrate Fair Information Practice Principles directly into the design and operation of privacy-enhancing technologies and the information management practices of organizations, have steadily given rise to a range of standardized tools and methodologies.

Privacy Self-Assessment Tools: Assessment tools help organizations understand and document current data holdings and flows, as well as operational states and processes, in a principled, systematic way. Self-assessment tools are fairly preliminary, often taking the form of structured checklists to help organizations determine their privacy "readiness," with preliminary guidance on how to systematically identify and address gaps. Many assessment tools serve as necessary foundations for privacy planning, action, and change,[13] and as benchmarks against which organizational progress may be measured, reported, and verified.[14]

[13] Examples include: IPC, Guardent & PricewaterhouseCoopers, *Privacy Diagnostic Tool* (2001); Office of the Privacy Commissioner of Canada [OPCC], 2004; American Institute of Certified Public Accountants/Canadian Institute of Chartered Accountants [AICPA/CICA], *Privacy Assessment Tool Version 2.0* (2010b).

[14] Examples include: AICPA/CICA *Privacy Maturity Model*; ISO/IEC 29100:2011 *Information technology – Security techniques – Privacy framework* (2010a).

Privacy Impact Assessments (PIAs): Canada is a world leader in developing and adopting PIAs, which are mandatory in the Ontario (provincial) and Canadian (federal) public sectors in order to receive program funding. Being proactive and systematic, PIAs are central to the *Privacy by Design* approach and for demonstrating due diligence in identifying and mitigating privacy and data protection risks associated with new data processing initiatives, projects, and other material changes in operating methods. They have caught on in public sectors around the world as a best practice, and are now being adapted for use throughout the private sector. PIA methodologies vary considerably in application, breadth, timing, transparency, and levels of prescription, among other dimensions.[15] A significant milestone in the development and adoption of PIAs was the industry-led RFID PIA Framework approved by the EU in 2011 for demonstrating "*Privacy by Design*" compliance with the *EU Data Protection Directive*. Privacy impact assessment methodologies and associated guidance documents have multiplied around the world.[16]

Risk Management: To be practical, efficient and effective, data protection needs to focus and prioritize resources on areas of highest risk. Indeed, privacy risk identification and mitigation strategies are central to good PIAs. Fortunately, standardized risk management methods are being developed and recognized internationally. For example, the Privacy Risk Optimization Process (PROP) is a methodology based on the International Organization for Standardization (ISO) concept that enables privacy and data protection risk mitigation efforts to be effectively integrated into operational policies and procedures.[17]

Privacy Management Frameworks: Systematic, verifiable methods for integrating privacy and security objectives and requirements into information technologies, organizational processes, and networked architectures are also emerging and maturing. Privacy management frameworks are the most comprehensive and detailed of methodologies for "resolving privacy policy requirements into operational privacy services and functions" and for establishing effective *internal* controls and accountability.[18] Concurrently, information *security* system standards and frameworks are being applied today by enterprises in greater numbers and with greater rigour, and Enterprise Architecture design has burgeoned as a discipline during the past decade,

[15] See Linden Consulting, Inc., Privacy Impact Assessments: International Study of their Application and Effects, prepared for Information Commissioner's Office United Kingdom (2007).

[16] Office of the Privacy Commissioner of Canada [OPCC] (2007), ICO (2007, 2009a, b), Office of the Privacy Commissioner of Australia [OPCA] (2010).

[17] See IPC, Ontario Lottery and Gaming Corporation and YMCA Canada (2009). Privacy Risk Management: Building privacy protection into a Risk Management Framework to ensure that privacy risks are managed, by default. See also Cavoukian and McQuay (2010).

[18] See International Security, Trust and Privacy Alliance (ISTPA) *Privacy Framework v1.1* (2002); OASIS *Privacy Management Reference Model 2.0* (2009); NIST 800-53 *Security and Privacy Controls for federal information systems and Organizations, Appendix* J (Privacy Controls, Enhancements, and Supplemental Guidance) (2012).

fueled in part by regulatory and competitive pressures. These information management efforts are consistent with, and can in most cases help inform and advance, *Privacy by Design* Principles.[19]

In the United States, the Federal Trade Commission (FTC) has begun to require some organizations to put in place comprehensive data protection programs that are auditable. In the European Union, "prior checking" and other due diligence requirements are becoming mandatory for organizations to proactively demonstrate compliance with privacy laws.

8.4.3.3 Full Functionality – Positive-Sum Not Zero-Sum (Practical & Demonstrable Results)

As noted above, privacy is not an absolute value. To design practical yet effective privacy and data protection in a given information technology, organization, or networked architecture, privacy solution architects typically need to take into account multiple legitimate (and, yes, sometimes competing) interests, and accommodate them in optimal, innovative ways.

The *PbD* Principle of *Full Functionality* requires going beyond making privacy declarations and data protection commitments, to *demonstrating* how all data processing and other objectives have been, and are being, satisfied. External accountability and leadership are enhanced by the application of this Principle, which emphasizes transparency and measurable outcomes.

- When embedding privacy and data protection into a given information technology, process, system, or architecture, it should be done in such a way that full functionality is not impaired, and that all legitimate interests are accommodated and requirements optimized.
- Privacy and data protection are often positioned in a zero-sum manner; that is, as having to compete with other legitimate interests, design objectives, and technical capabilities in a given domain. *Privacy by Design* rejects taking such an approach – it embraces legitimate non-privacy objectives and accommodates them in an innovative positive-sum manner.
- All interests and objectives must be clearly documented, desired functions articulated, metrics agreed upon and applied, and unnecessary trade-offs rejected, in favour of finding a solution that enables multi-functionality.

Additional recognition is garnered for creativity and innovation in achieving all objectives and functionalities in an integrative, positive-sum manner. Entities that succeed in overcoming outmoded zero-sum choices are demonstrating global privacy leadership.

[19] See Abrams and Taylor (2010), Centre for Information Policy Leadership [CIPL] (2009, 2010), European Commission [EC] (2010c).

This Principle challenges policymakers, executives, technologists, and designers, among others, to find ways to achieve better privacy and data protection in a given technology, system, or domain than is currently the case, or being proposed, and to be able to document and demonstrate achievements so that others may learn from them and they become best practices.

Certain kinds of privacy and security technologies, such as encryption, access control, and auditing tools, are easy to promote because the data protection benefits of using them are self-evident and tend to outweigh the perceived costs. Legal requirements, such as mandatory breach notification and contractual agreements, also provide additional incentives to proactively develop and adopt privacy-enhancing technologies.

There are many examples of positive-sum "transformative" technologies that achieve multiple objectives in a privacy-enhancing manner. One is Biometric Encryption (BE), which achieves positive identification without the need for centrally-stored templates. BE has been successfully deployed across Ontario gaming facilities to identify gamblers who have requested to be barred from entering the premises.[20] Two other technologies are: privacy-enhanced road toll pricing, which enables vehicle tracking and billing in a way that minimizes or even excludes third-party access to the detailed location and usage data; and smart meters, which accomplish similar objectives with respect to household energy consumption patterns.[21] Thirdly, the simple addition of user-controlled on-off switches for RFID-embedded identity and other smart cards, helps defeat unwanted surveillance, tracking, and other abuses of these unique identity beacons by ensuring that the default mode of operation is *off* until users take the affirmative step of turning it on for data transmission and use.[22]

Privacy-enhanced IT products and services are being certified in Europe by EuroPriSe, a consortium led by the Independent Centre for Privacy Protection Schleswig-Holstein. In 2007, EuroPriSe introduced a European Privacy Seal for IT products and IT-based services that have proven privacy compliance under European data protection law in a two-step independent certification procedure. The program offers evaluations and certifications according to the European Privacy Seal procedure to any vendor or service provider that applies. The privacy certificate aims to facilitate an increase in market transparency for privacy-relevant products, and an enlargement of the market for privacy-enhancing technologies – and ultimately, an increase in trust in IT. The EuroPriSe certificate has been awarded to nearly 20 IT products and services to date.[23] Similar privacy "trustmark" programs are also

[20] See Ann Cavoukian and Tom Marinelli (2010) Privacy-Protective Facial Recognition: Biometric Encryption Proof of Concept.

[21] See IWGDPT (2011) Privacy by Design and Smart Metering: Minimize Personal Information to Maintain Privacy, Working Paper 675.43.18 and (2009) Report and Guidance on Road Pricing – "Sofia Memorandum" 675.38.12. and Carmel Troncoso et al. (2011) "PriPAYD: Friendly Pay-As-You-Drive Insurance", in *IEEE Transactions on Dependable and Secure Computing.*

[22] See Ann Cavoukian (2009e).

[23] EuroPriSe European Privacy Seal awards at www.european-privacy-seal.eu/awarded-seals.

underway elsewhere, reflecting interest and growth in independent audit, evaluation, and certification methods.[24]

The creation, recognition, and adoption of PETs as a means to achieve *Privacy by Design* design and operational goals is being actively promoted by the European Commission, not only as a major ongoing research funding initiative under the Framework Programme,[25] but notably in the context of the current EU review of, and proposed amendments to, the *Data Protection Directive*.[26]

Current work by international data protection authorities on defining accountability is also establishing common definitions and best practices that can advance organizational *Privacy by Design* practices.[27] Similar work is also underway in international standards groups to define privacy implementation and assessment methodologies. The preparation, use, and publication – whether mandatory, contractual, or voluntary – of Privacy Impact Assessments and privacy management frameworks, are also on the rise.[28] We are seeing the emergence and growth of standardized privacy evaluation, audit, and assurance systems, such as the Generally Accepted Privacy Principles (GAPP), innovative co-regulatory initiatives, certification seals and trustmarks (e.g., EuroPriSe), and other criteria. Enhanced diligence and accountability measures are consistent with a *Privacy by Design* approach to demonstrating results. The publication of successful case studies adds illustrative and educational value, and examples for others to follow.[29]

Perhaps the most exciting chapters on achieving *Privacy by Design* results have yet to be written, as public policymakers on both sides of the Atlantic Ocean actively propose weaving the *Privacy by Design* approach and Principles into the fabric of revised privacy laws, and in strengthened systems of regulatory oversight.[30]

8.5 The Challenges Ahead

It has become trite to observe that data is the lifeblood of the new economy, but who today can truly grasp how large the arteries are becoming, how they are multiplying, where they may lead, and to what end? Thanks to new information flows, today we

[24] For example, Japan's *PrivacyMark*, AICPA/CICA's *WebTrust*, and *EBTrust* in Norway.

[25] See list of European Commission-funded projects, ICT Research in FP7, Research activities in trust, privacy and identity in the digital economy at: http://cordis.europa.eu/fp7/ict/security/projects_en.html.

[26] European Commission (2007, 2009, 2010a, b, c, 2011).

[27] Galway Project (2009), "Paris" Project (2010).

[28] See PIA resources in Bibliography.

[29] See www.privacybydesign.ca for extensive *PbD* resources and case studies.

[30] FTC (2010), EC (2010a, b, c, 2011a, b, 2012).

enjoy unprecedented and nearly unimaginable new services and benefits. But these have been accompanied by unprecedented and previously unimaginable privacy threats and harms. It is essential that methods to ensure confidence and trust in the information economy are established.

- **Bridging the Accountability Gap**: The need for organizational accountability remains constant – indeed, it is more urgent today than ever before. As organizational business models, structures, and methods of operation evolve, the means by which accountability is demonstrated internally, and to individuals, regulators, and business partners, must also evolve. Beyond policy statements, promises, and contractual terms, what is needed now are more innovative and robust methods to assure all stakeholders that personal data is, in fact, being managed responsibly.
- **Prevention First – Do No Harm**: In recent years there has been increasing emphasis on *prevention* as a distinct privacy principle, reflecting a growing international consensus that it is better to prevent foreseeable harms from occurring in the first place than to remediate them after the fact. This trend has been accompanied by a shift to organizations in responsibility for anticipating and reducing the likelihood of undesirable effects at every stage of data processing.
- **Establishing Privacy Standards and Implementation Methodologies**: We are seeing the emergence and establishment of more standardized and systematic methods for ensuring that privacy and data protection are, indeed, being built into the operation of data processing technologies and systems. Regulators, commissioners, data protection authorities, attorneys-general, and others are demanding stronger evidence that privacy and data protection promises are being kept and that due diligence is being applied – preferably via methods that are amenable to external review and validation. The phenomenal growth in chief privacy officer-type positions, roles, and functions in the past decade reflects the response of organizations to demand for expertise in applying privacy methods.
- **Developing Privacy and Assurance Metrics**: We are also seeing broader-based demand for assurance, trust signals, and other metrics that can convey adherence to privacy standards in a way that is clear and meaningful to all stakeholders. In many respects, privacy protection as a formal discipline is in a relative state of infancy, somewhat like information security was 10–15 years ago: in need of greater standardization of definitions, implementation methods, control objectives, and metrics.
- **Enhancing Privacy Management and Governance Frameworks**: There are many paths to enhanced accountability for privacy and data protection, typically involving a mix of technology, policies and practices, and "smart" regulation. More than ever, a comprehensive *Privacy by Design* approach to information management is called for – one which assures end-to-end chain of custody and responsibility, from the very start.
- The scale and complexity of current data systems, networks, and practices require a new and updated set of universally-accepted privacy design and practice principles that are comprehensive, robust, and capable of assuring privacy protection, confidence, and trust amid the new global realities.

- **Expanding Domains and Scopes of Application**: In recent years, it has become clear that a *Privacy by Design* approach can and should be applied to the broader information ecosystems in which both technologies and organizations are embedded and must function. Privacy and data protection benefit from taking a holistic, integrative approach that considers as many contextual factors as possible – even (or especially) when these factors lie outside the direct control of any particular actor, organization, or component in the system.

A broader, architectural view is ideal. It makes sense to ask how the *Privacy by Design* Foundational Principles and the *PbD* approach could be applied to overarching information architectures, platforms, and interoperable networks such as: federated identity systems,[31] online social networks[32] and other "Web 2.0" phenomena,[33] e-Government,[34] behavioural advertising networks and systems, cloud computing,[35] location-based services, the "Internet of Things," Internet protocols, and even "smart" systems of regulation.[36]

Globalized privacy challenges require a global approach, global cooperation, and global solutions. Leadership is essential to articulate and pursue the highest possible privacy ideals and standards possible. In addition, design methods and systems must be created for ensuring these ideals are driven through the information architectures and ecosystems in a coordinated manner, and to demonstrate innovative, concrete, real-world, practical, measurable "win-win" results.

8.6 Conclusions

With the shift from industrial manufacturing to knowledge creation and service delivery, the value of information and the need to manage it responsibly have grown dramatically. At the same time, rapid innovation, global competition, and increasing system complexity present profound challenges for informational privacy and data protection.

While we would like to enjoy the benefits of innovation – new conveniences and efficiencies – we must also preserve freedom of choice and personal control over personal data flows. Always a social norm, privacy and data protections have nonetheless evolved over the years, beyond being viewed solely as a legal compliance requirement, to being recognized as a market imperative and critical enabler of trust and freedoms in our present-day information society.

---

[31] Cameron (2005), Cavoukian and Tapscott (2006, Cavoukian 2009b), Cameron et al. (2008), European Network and Information Security Agency [ENISA] (2009), U.S. White House (2010).

[32] International Working Group on Data Protection in Telecommunications [IWGDPT] (2008).

[33] Cavoukian (2008a).

[34] Cavoukian (2009a, b, c, d, e).

[35] NEC (2010).

[36] Cavoukian (2009a, b, c, d, e), Schwartz et al. (2007), CIPPIC (2007), Romanosky et al. (2011).

There is a growing understanding that innovation and competitiveness must be approached from a "design-thinking" perspective – namely, a way of viewing the world and overcoming constraints that is at once holistic, interdisciplinary, integrative, creative, innovative, and inspiring.

Privacy, too, must be approached from the same design-thinking perspective. Privacy and data protections should be incorporated into networked data systems and technologies by default, and become integral to organizational priorities, project objectives, design processes, and planning operations. Ideally, privacy and data protection should be embedded into every standard, protocol, and data practice that touches our lives.

We have also seen how the *PbD* Foundational Principles represent an evolution of traditional principles of Fair Information Practices, incorporating FIPPs but going beyond them to encompass the requirements for proactive leadership, verifiable methods, and demonstrable, positive-sum results.

Privacy by Design is on the cusp of becoming a regulatory requirement in two major jurisdictions, but there remains much work ahead in defining its requirements more precisely, according to each domain and scope of application. *PbD* will continue to evolve as it is adopted around the world and adapted to a myriad of circumstances and needs, giving us cause to be both hopeful and confident that a strong basis has been established for the survival of privacy well into the twenty-first century, and beyond.

Acknowledgement I gratefully acknowledge the work of Fred Carter, Senior Policy & Technology Advisor, Office of the Information and Privacy Commissioner of Ontario, Canada, in the preparation of this paper.

References

American Institute of Certified Public Accountants (AICPA) and Canadian Institute of Chartered Accountants (CICA). 2010a. *Generally Accepted Privacy Principles (GAPP) and Criteria and the AICPA/CICA PRIVACY MATURITY MODEL Based On Generally Accepted Privacy Principles*. http://bit.ly/ePrxwg and http://bit.ly/fQVes1, respectively. Accessed 13 Jan 2012.

American Institute of Certified Public Accountants (AICPA) and Canadian Institute of Chartered Accountants (CICA). 2010b. *AICPA CICA Privacy Assessment Tool Version 2.0.* http://tinyurl.com/cap7fsp. Accessed 12 Mar 2012.

Bennett, Colin J. 2009. International privacy standards: A continuing convergence. http://bit.ly/hBk3oX. Accessed 13 Jan 2012.

Cameron, Kim. 2005. The laws of identity, identity blog. http://bit.ly/eAHmWu. Accessed 13 Jan 2012.

Cameron, Kim, Posch Reinhard, and Rannenberg Kai. 2008. Proposal for a common identity framework: A user-centric identity metasystem. http://bit.ly/i6lAfE. Accessed 13 Jan 2012.

Canadian Internet Policy and Public Interest Clinic (CIPPIC). 2007. Approaches to security breach notification: A white paper. http://bit.ly/fqzEQ6. Accessed 13 Jan 2012.

Cavoukian, Ann, Information and Privacy Commissioner of Ontario, Canada

Cavoukian, Ann. 2002. Security technologies enabling privacy (STEPs): Time for a paradigm shift. Office of the Information and Privacy Commissioner of Ontario, Canada. http://bit.ly/fjpfrt. Accessed 13 Jan 2012.

Cavoukian, Ann. 2008a. Privacy in the Clouds, *Identity in the Information Society*, 1: 89–108. 2008. And Privacy in the clouds: Privacy and digital identity: Implications for the Internet. Office of the Information and Privacy Commissioner of Ontario, Canada. http://bit.ly/gWH3cu and http://bit.ly/gWuD7V, respectively. Accessed 13 Jan 2012.

Cavoukian, Ann. 2008b. Privacy & radical pragmatism: Change the paradigm. Office of the Information and Privacy Commissioner of Ontario, Canada. http://bit.ly/h1MT9W. Accessed 13 Jan 2012.

Cavoukian, Ann. 2008c. RFID and privacy: Guidance for health-care providers. Office of the Information and Privacy Commissioner of Ontario, Canada. http://bit.ly/Oj6CDn. Accessed 13 Jan 2012.

Cavoukian, Ann. 2009a. Moving forward from PETs to PETs plus: The time for change is now. Office of the Information and Privacy Commissioner of Ontario, Canada. http://bit.ly/fkeHt8. Accessed 13 Jan 2012.

Cavoukian, Ann. 2009b. Transformative technologies deliver both security and privacy: Think positive-sum not zero-sum. Office of the Information and Privacy Commissioner of Ontario, Canada. http://bit.ly/dTi0jh. Accessed 13 Jan 2012.

Cavoukian, Ann. 2009c. Privacy and government 2.0: The implications of an open world. Office of the Information and Privacy Commissioner of Ontario, Canada. http://bit.ly/f7kHAn. Accessed 13 Jan 2012.

Cavoukian, Ann. 2009d. A discussion paper on privacy externalities, security breach notification and the role of independent oversight. Office of the Information and Privacy Commissioner of Ontario, Canada. http://bit.ly/gdtufG. Accessed 13 Jan 2012.

Cavoukian, Ann. 2009e. *Adding an on/off device to activate the RFID in enhanced driver's licences: Pioneering a made-in-Ontario Transformative Technology that delivers both privacy and security*. Canada: Office of the Information and Privacy Commissioner of Ontario. http://bit.ly/fbSbpl. Accessed 13 Aug 2012.

Cavoukian, Ann. 2009, rev. 2011. *Privacy by Design*: The 7 foundational principles. Office of the Information and Privacy Commissioner of Ontario, Canada. http://bit.ly/gwzJgw. Accessed 13 Jan 2012.

Cavoukian, Ann. 2012. *Privacy by Design*: Origins, meaning, and prospects for assuring privacy and trust in the information era. In *Privacy protection measures and technologies in business organizations: Aspects and standards*, George O.M. Yee, ed. Ottawa: Aptus Research Solutions Inc. and Carleton University. doi: 10.4018/978-1-61350-501-4, ISBN13: 9781613505014, ISBN10: 1613505019, EISBN13: 9781613505021.

Cavoukian, Ann. (Joint Publications)

Cavoukian, Ann, and Tapscott, Don. 2006. Privacy and the open-networked enterprise. Office of the Information and Privacy Commissioner of Ontario, Canada. http://bit.ly/eTdiya. Accessed 13 Jan 2012.

Cavoukian, Ann, and McQuay, Terry. 2010. A pragmatic approach to privacy risk optimization: *Privacy by Design* for business practices. *Identity in the Information Society* 3: 405–413. http://bit.ly/hC7hED. Accessed 13 Jan 2012.

Cavoukian, Ann, Abrams Marty, and Taylor Scott. 2010. *Privacy by Design*: Essential for organizational accountability and strong business practices. *Identity in the Information Society* 3: 405–413. http://bit.ly/dOJYOc. Accessed 13 Jan 2012.
Cavoukian, Ann, and Marinelli Tom. 2010 Privacy-protective facial recognition: Biometric encryption proof of concept. http://tinyurl.com/dxhh5x6. Accessed 14 Mar 2012.

Centre for Information Policy Leadership (CIPL) as Secretariat to the "Galway" and "Paris" Projects

CIPL. 2009. Data protection accountability: The essential elements: A document for discussion. http://1.usa.gov/hvlZcD. Accessed 13 Jan 2012.
CIPL. 2010. Demonstrating and measuring accountability a discussion document accountability Phase II – The Paris Project. http://bit.ly/gRFrob. Accessed 13 Jan 2012.
Cuijpers, Colette. 2007. A private law approach to privacy; Mandatory Law, 4:4 SCRIPTed 318. www.law.ed.ac.uk/ahrc/script-ed/vol4-4/cuijpers.asp. Accessed 14 Mar 2012.

European Commission (EC)

EC. 2009. The future of privacy: Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data, Article 29 Data Protection Working Party, WP 168. http://bit.ly/gWJ56l. Accessed 13 Jan 2012.
EC. 2010a. Communication from the commission to the European parliament, the council, the economic and social committee and the committee of the regions: A comprehensive approach on personal data protection in the European Union. Technical report. http://bit.ly/grpr4w. Accessed 13 Jan 2012.
EC. 2010b. Study on the economic benefits of privacy-enhancing technologies, Final Report to The European Commission, DG Justice, Freedom and Security. http://bit.ly/heQNQT. Accessed 13 Jan 2012.
EC. 2010c. Opinion 3/2010 on the principle of accountability, Article 29 Data Protection Working Party, WP 173. http://bit.ly/eEFeaq. Accessed 13 Jan 2012.
EC. 2012. EU Commission proposes a comprehensive reform of the data protection rules, Press Release, DG Justice. http://tinyurl.com/7bylsks. Accessed 26 Mar 2012.
European Network and Information Security Agency (ENISA). 2009. Privacy and e-ID: Press release and position paper. http://bit.ly/dNNRD6. Accessed 13 Jan 2012.
Fischer-Hübner, Simone, Hoofnagle Chris, Rannenberg Kai, Waidner Michael, Krontiris Ioannis, and Marhöfer Michael. 2011. Online privacy: Towards informational self-determination on the Internet. Dagstuhl Perspectives Workshop 11061. doi: 10.4230/DagRep.1.2.1. http://drops.dagstuhl.de/opus/volltexte/2011/3151/. Accessed 17 Jun 2011.
Ford, R. 2004. Beware rise of Big Brother state, warns data watchdog. *The Times* 16 August 2004. http://thetim.es/hw1abr. Accessed 12 Dec 2012.

International Conference of Privacy and Data Protection Commissioners (ICPDPC)

ICPDPC. 2010. *Privacy by Design* resolution, adopted at Jerusalem, Israel, October 27–29, 2010. http://bit.ly/fffv0l. Accessed 13 Jan 2012.

International Working Group on Data Protection in Telecommunications (IWGDPT)

András Jóri. 2007. Data protection law – An introduction. www.dataprotection.eu/pmwiki/pmwiki.php?n=Main.Privacy. Accessed on 14 Mar 2012.

IWGDPT. 2008. Report and guidance on privacy in social network services – Rome Memorandum, 675.36.5. http://bit.ly/er5SjW. Accessed 13 Jan 2012.

IWGDPT. 2009. Report and guidance on road pricing – Sofia Memorandum, 675.38.12. http://www.datenschutz-berlin.de/attachments/647/WP_Road_Pricing_Final_675.38.12.pdf. Accessed 14 Mar 2012.

IWGDPT. 2011. *Privacy by Design* and smart metering: Minimize personal information to maintain privacy. Working Paper 675.43.18. www.datenschutz-berlin.de/attachments/842/675.43.18_WP_Privacy_and_Smart_Metering.pdf. Accessed 14 Mar 2012.

Mayer-Schönberger, Viktor. 1997. Generational development of data protection in Europe. In *Technology and privacy: The new landscape*, ed. Philip Agre and Marc Rotenberg, 219–41. Cambridge, MA: MIT Press.

Office of the Information and Privacy Commissioner of Ontario, Canada. (Joint Publications)

Office of the Information and Privacy Commissioner of Ontario, Canada, NEC Computing. 2010. Modelling cloud computing architecture without compromising privacy: A *Privacy by Design* approach. Office of the Information and Privacy Commissioner of Ontario, Canada. http://bit.ly/fqnA8v. Accessed 13 Jan 2012.

Office of the Information and Privacy Commissioner of Ontario, Canada, and Nymity. 2010. A pragmatic approach to privacy risk optimization: *Privacy by Design* for business practices. Office of the Privacy Commissioner of Ontario, Canada. http://bit.ly/hl0ws8. Accessed 13 Jan 2012.

Office of the Information and Privacy Commissioner of Ontario, Canada, Guardent and PricewaterhouseCoopers. 2001. Privacy diagnostic tool workbook and FAQ. Office of the Information and Privacy Commissioner of Ontario, Canada. http://bit.ly/gAhbsN and http://bit.ly/eaHrMv, respectively. Accessed 13 Jan 2012.

Office of the Information and Privacy Commissioner of Ontario, Canada, Ontario Lottery and Gaming Corporation & YMCA Canada. 2009a. Privacy risk management: Building privacy protection into a risk management framework to ensure that privacy risks are managed, by default. Office of the Information and Privacy Commissioner of Ontario, Canada. http://bit.ly/gGMA4r. Accessed 13 Jan 2012.

Office of the Information and Privacy Commissioner of Ontario,Canada and Liberty Alliance. 2009. *The New Federated Privacy Impact Assessment(F-PIA) bulding privacy and trust-enabled federation*. Canada: Office of the Informationa and Privacy Commissioner of Ontario. http://bit.ly/f89UMs. Accessed 13 Aug 2012.

Office of the Privacy Commissioner of Australia (OPCA). 2010. Privacy Impact Assessments (PIA) guide. http://bit.ly/hRQu0a. Accessed 13 Jan 2012.

Office of the Privacy Commissioner of Canada (OPCC)

OPCC. 2004. A guide for businesses and organizations: Your privacy responsibilities. Office of the Privacy Commissioner of Canada. http://bit.ly/fRKncL. Accessed 13 Jan 2012.

OPCC. 2007. Fact sheet on PIAs. Office of the Privacy Commissioner of Canada. http://bit.ly/dTZ8Aj. Accessed 13 Jan 2012.

Ponemon Institute, The:

Ponemon Institute. 2010. 2009 annual study: Cost of a privacy breach sponsored by PGP Corp. http://bit.ly/eRxyMK. Accessed 13 Jan 2012.
Ponemon Institute. 2011. The true costs of compliance: A benchmark study of multinational organizations, independent research report. http://bit.ly/e13LZT. Accessed 13 Jan 2012.
Privacy International. 1998–2003. Privacy and human rights, annual reports. http://bit.ly/hjKLSe. Accessed 13 Jan 2012.
Privacy International and the Electronic Privacy Information Center (EPIC). 2007. Privacy and human rights 2006: An international survey of privacy laws and developments. http://bit.ly/g9wOAh. Accessed 13 Jan 2012.
Privacy International, the Electronic Privacy Information Center (EPIC) and the Center for Media and Communications Studies (CMCS). 2011. European privacy and human rights 2010. http://bit.ly/gnFZoC. Accessed 13 Jan 2012.
Romanosky, Sasha, Rahul Telang, and Alessandro Acquisti. 2011. Do data breach disclosure laws reduse identity theft? *Journal of Policy Analysis and Management* 30(2): 256–286. Available at SSRN: http://ssrn.com/abstract=1268926
Schwartz, Paul M., and Janger Edward J. 2007. Notification of data security breaches. *Michigan Law Review* 105: 913. Brooklyn Law School, Legal Studies Paper No. 58. http://bit.ly/hQjHT0. Accessed 13 Jan 2012.
Troncoso, Carmela, Danezis George, Kosta Eleni, Balasch Joseph, and Preneel Bart. 2011. PriPAYD: Friendly pay-as-you-drive insurance. *IEEE Transactions on Dependable and Secure Computing* 8(5): 742–755. Accessible at: www.cosic.esat.kuleuven.be/publications/article-2013.pdf.

U.K. Information Commissioner's Office (ICO)

U.K. Information Commissioner's Office (ICO). 2007. An international study of PIA law, policies and practices, ICO. http://bit.ly/hB381i. Accessed 13 Jan 2012.
U.K. Information Commissioner's Office (ICO). 2009a. Protecting people: A data protection strategy for the Information Commissioner's Office. ICO. http://bit.ly/gi5vW1. Accessed 13 Jan 2012.
U.K. Information Commissioner's Office (ICO). 2009b. PIA Handbook, ICO. http://bit.ly/eEKU06. Accessed 13 Jan 2012.
U.S. Federal Trade Commission (FTC). 2010. Protecting consumer privacy in an era of rapid change: A proposed framework for businesses and policymakers. Staff technical report. http://1.usa.gov/eupYzF. Accessed 13 Jan 2012.
U.S. White House. 2010. Draft national strategy for trusted identities in cyberspace: Creating options for enhanced online security and privacy. http://1.usa.gov/hNs1jw. Accessed 13 Jan 2012.

Additional Readings

Borking, J.J. 2005. Privacy standards for trust. Presentation to the London conference of Data Protection Authorities. http://bit.ly/gTjOVq. Accessed 13 Jan 2012.
Borking, J.J., and Raab, C. 2001. Laws, PETS and other technologies for privacy protection. *Journal of Information, Law and Technology* 1, pp. 1–14.http://bit.ly/PkslMr.

Cavoukian, A, Information and Privacy Commissioner, Ontario, Canada

Cavoukian, A. May 2011. *Privacy by ReDesign*: Building a better legacy. Available at: www.privacybydesign.ca
Cavoukian, A. Aug 2011. *Privacy by Design* in law, policy and practice: A white paper for regulators, decision-makers and policy-makers.
Cavoukian, A. Sept 2011. *Privacy by Design*: From policy to practice.
Cavoukian, A. Nov 2011. *Privacy by ReDesign*: A practical framework for implementation.

Center for Democracy and Technology (CDT)

CDT. 2009a. Perspective on *PbD*. http://bit.ly/fuxn0t. Accessed 13 Jan 2012.
CDT. 2009b. The role of Privacy by Design in protecting consumer privacy. Comments submitted to the FTC Consumer Privacy Roundtable. http://1.usa.gov/eMH4jv. Accessed 13 Jan, 2012.
Computers, Privacy and Freedom (CFP). 2000, April. *Privacy by Design* workshop proceedings. Toronto, Ontario, Canada. http://bit.ly/e5UegE. Accessed 13 Jan 2012.
Dutch Data Protection Agency. 2004. Privacy-enhancing technologies. White paper for decision-makers. http://bit.ly/dFRV8q. Accessed 13 Jan 2012.

European Commission (EC)

EC. 2007a. European Commission supports PETs: Promoting data protection by Privacy Enhancing Technologies, Press Release. http://bit.ly/epnO5w. Accessed 13 Jan 2012.
EC. 2007b. Communication from the commission to the European parliament and the council on promoting data protection by privacy enhancing technologies (PETs), COM(2007) 228 final. Brussels, 2.5.2007 and Background Memo. http://bit.ly/hRdu8n and http://bit.ly/gF8BhA, respectively. Accessed 13 Jan 2012.
EC. 2009. The future of privacy: Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data, Article 29 Data Protection Working Party, WP 168. http://bit.ly/gWJ56l. Accessed 13 Jan 2012.
EC. 2010a. Opinion 5/2010 on the Industry Proposal for a Privacy and Data Protection Impact Assessment Framework for RFID Applications, Article 29 Data Protection Working Party, WP175. http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp175_en.pdf.
EC. 2010b. Communication from the commission to the European parliament, the council, the economic and social committee and the committee of the regions: A comprehensive approach on personal data protection in the European Union. Technical report. http://bit.ly/grpr4w. Accessed 13 Jan 2012.
EC. 2010c. Study on the economic benefits of privacy-enhancing technologies, Final Report to The European Commission, DG Justice, Freedom and Security. http://bit.ly/heQNQT. Accessed 13 Jan 2012.
EC. 2010d. Opinion 3/2010 on the principle of accountability, Article 29 Data Protection Working Party, WP 173. http://bit.ly/eEFeaq. Accessed 13 Jan 2012.
EC. 2011a. Opinion 9/2011 on the revised Industry Proposal for a Privacy and Data Protection Impact Assessment Framework for RFID Applications, Article 29 Data Protection Working Party, WP180. http://cordis.europa.eu/fp7/ict/enet/documents/rfid-pia-framework-a29wp-opinion-11-02-2011_en.pdf.

EC. 2011b. Privacy and data protection impact assessment framework for RFID applications. http://ec.europa.eu/information_society/policy/rfid/documents/infso-2011-00068.pdf.
European Council. Feb 2011. Council conclusions on the Communication from the Commission to the European Parliament and the Council – A comprehensive approach on personal data protection in the European Union, 3071st JUSTICE and HOME AFFAIRS Council meeting, Brussels. http://bit.ly/gx4wS0. Accessed 13 Jan 2012.

European Commission-funded initiatives

European Commission-funded initiatives: FIDIS Project. 2007. Identity and impact of privacy enhancing technologies. http://bit.ly/e8A0aG. Accessed 13 Jan 2012.
European Commission-funded initiatives: PISA Project. 2003. Handbook of privacy-enhancing technologies – The case of intelligent software agents. The Hague. http://bit.ly/f32fns. Accessed 13 Jan 2012.
European Commission-funded initiatives: PRIME Project. 2007. PRIME White paper v2. http://bit.ly/hry9Og. Accessed 13 Jan 2012.
EU Privacy Impact Assessment Observatory: http://www.piawatch.eu/
EU Privacy Impact Framework project: www.piafproject.eu
European Network and Information Security Agency (ENISA). 31 Mar 2010. Opinion on the industry proposal for a privacy and data protection impact assessment framework for RFID applications. http://www.enisa.europa.eu/media/news-items/enisa-opinion-on-pia.
Gürses, S., C. Troncoso, and C. Diaz. 2011. *Engineering Privacy by Design*. https://www.cosic.esat.kuleuven.be/publications/article-1542.pdf. Accessed 14 Feb 2012.)

Hustinx, P., European Data Protection Supervisor (EDPS)

Hustinx, P., and EDPS. 2008, April. EDPS issues policy paper on his role in EU research and technological development, Press Release. http://bit.ly/hKCs5x. Accessed 13 Jan 2012.
Hustinx, P., and EDPS. 2010a, March. Opinion of the European Data Protection Supervisor on Promoting Trust in the Information Society by Fostering Data Protection and Privacy, EDPS. http://bit.ly/h9qzmP. Accessed 13 Jan 2012.
Hustinx, P., and EDPS. 2010b, March. Press Release, EDPS opinion on privacy in the digital age: "Privacy by Design" as a key tool to ensure citizens' trust in ICTs, EDPS/10/6. http://bit.ly/hNJDZy. Accessed 13 Jan 2012.
Initiative for Privacy Standardization in Europe (IPSE), European Committee for Standardization (CEN). 2002. Final Report of the EU CEN/ISSS Initiative on Privacy Standardization in Europe. http://bit.ly/hZX7io. Accessed 13 Jan 2012.
International Working Group on Data Protection in Telecommunications (IWGDPT). 2011. Privacy by Design and smart metering: Minimize personal information to maintain privacy, 675.43.18. http://goo.gl/2zld1. Accessed 14 Feb 2012.

International Security, Trust and Privacy Alliance (ISTPA)

ISTPA. 2007. Analysis of privacy principles: Making privacy operational. http://bit.ly/gZu2pm. Accessed 13 Jan 2012.

ISTPA. 2009. Privacy management reference model 2.0 v.2.0: A framework for resolving privacy policy requirements into operational privacy services and functions. http://bit.ly/dUMaiD. Accessed 13 Jan 2012.
Kenny, S., and Borking, J. 2002. 'The Value of Privacy Engineering', Refereed Article, *The Journal of Information, Law and Technology* (JILT) 2002 (1). http://bit.ly/gk9P3E. Accessed 13 Jan 2012.
London Economics. 2010. Study on the economic benefits of privacy-enhancing technologies, Final Report to The European Commission, DG Justice, Freedom and Security. http://bit.ly/heQNQT. Accessed 13 Jan 2012.
Microsoft Corp. 2006. Privacy guidelines for developing software products and services. http://bit.ly/ijIMVk. Accessed 13 Jan 2012.

Organisation for Economic Co-operation and Development (OECD)

OECD. 2003. Directorate for Science, Technology and Industry, Committee for Information, Computer and Communications Policy, Inventory of privacy-enhancing technologies (PETs). http://bit.ly/hrFQIs. Accessed 8 Apr 2011.
OECD. 2008. At a Crossroads: "Personhood" and the digital identity in the information society. STI Working Paper 2007/7. http://bit.ly/gFBhlQ. Accessed 8 Apr 2011.
OECD. 2011a. Directorate for Science, Technology and Industry, Committee for Information, Computer and Communications Policy, The evolving privacy landscape: 30 years after the OECD privacy guideline. www.oecd.org/dataoecd/22/25/47683378.pdf. Accessed 16 Feb 2012.
OECD. 2011b. The 30th anniversary of the OECD privacy guidelines (web page) at www.oecd.org/sti/privacyanniversary
Rost, Martin, and Bock Kirsten. 2011. Privacy by Design and the new protection goals www.maroki.de/pub/privacy/BockRost_PbD_DPG_en_v1f.pdf. Accessed 14 Feb 2012.
Rubinstein, Ira S. 2011. Regulating Privacy by Design. http://goo.gl/WRCv5. Accessed 14 Feb 2012.
Spiekermann, Sarah, and Cranor, Lorrie Faith. 2009. Engineering privacy. *IEEE Transactions on Software Engineering* 35(1): 67–82. doi: 10.1109/TSE.2008.88.
Springer Publications. 2010. Special Privacy by Design issue of Identity in the Information Society 3(2). http://bit.ly/fo6l1q. Accessed 13 Jan 2012.
Tene, Omer. 2011. Privacy: The new generations. *International Data Privacy Law* 1(1): 15–27. doi:10.1093/idpl/ipq003. First published online: 5 Oct 2010.
U.K. Royal Academy of Engineering Society. 2007. Report: Dilemmas of privacy and surveillance: Challenges of technological change. http://bit.ly/gJUmJm – Press release: http://bit.ly/hSo1O0. Accessed 13 Jan 2012.

Wright, David

Wright, David. 2011a. Should privacy impact assessments be mandatory?. *Communications of the ACM* 54(8). http://cacm.acm.org/magazines/2011/8. Accessed Aug 2011.
Wright, David. 2011b. A framework for the ethical impact assessment of information technology. *Ethics and Information Technology* 13(3): 199–226. www.springerlink.com/content/nw5v71087x60/. Accessed Sept 2011.

Wright, David. 2012. The state of the art in privacy impact assessment. *Computer Law & Security Review* 28(1): 54–61. www.sciencedirect.com/science/journal/02673649. Accessed Feb 2012.

Wright, David, and Paul De Hert. 2012. *Privacy impact assessment*. Springer Law, Governance and Technology Series, Vol. 6. www.springer.com/law/international/book/978-94-007-2542-3.

Wright, David, Paul De Hert and Serge Gutwirth. 2011a. Are the OECD guidelines at 30 showing their age?. *Communications of the ACM* 54(2): 119–127. http://cacm.acm.org/magazines/2011/2. Accessed Feb 2011.

Wright, David, Gellert Raphaël, Gutwirth Serge and Friedewald Michael. 2011b. Minimizing technology risks with PIAs, precaution and participation. *IEEE Technology & Society*, 30(4):47–54, Winter 2011.

Chapter 9
Roadmap for Privacy Protection in Mobile Sensing Applications

Delphine Christin and Matthias Hollick

9.1 Introduction

Information and Communication Technology (ICT) is commonly seen as the key enabler for improving the quality of life in our modern society. For example, services such as eGovernment, have improved the efficiency of existing solutions and have successfully included citizens in the digital world. In a second wave, the technological advances of mobile phones promise a further diminution of the gap between physical world and cyberspace. A torrent of data about the physical world can be captured by using sensors embedded in mobile phones. The inclusion of the gathered data into the digital world contributes to the realization of the vision of so-called smart spaces, ranging from smart homes to smart cities and beyond. These smart spaces can substantially increase the quality of life by leveraging the citizens' participation by, e.g., monitoring traffic congestion[1] and noise pollution[2] in dense urban areas. The collection of sensor readings in mobile sensing applications however puts at risk the privacy of the users, as they may reveal sensitive information about themselves, such as the locations they visited.[3] Users aware of such threats may decide to

[1] Prashanth Mohan, Venkata N. Padmanabhan, and Ramachandran Ramjee, "Nericell: Rich Monitoring of Road and Traffic Conditions Using Mobile Smartphones," in *Proceedings of the 6th ACM Conference on Embedded Network Sensor Systems (SenSys)*, 2008.

[2] Rajib K. Rana et al., "Ear-Phone: An End-to-end Participatory Urban Noise Mapping System," in *Proceedings of the 9th ACM/IEEE International Conference on Information Processing in Sensor Networks (IPSN)*, 2010.

[3] Katie Shilton, "Four Billion Little Brothers?: Privacy, Mobile Phones, and Ubiquitous Data Collection," *Communications of the ACM* 52 (2009).

D. Christin (✉) • M. Hollick
Secure Mobile Networking Lab, Center for Advanced Security
Research Darmstadt (CASED), Technische Universität Darmstadt,
Mornewegstr. 32, 64293 Darmstadt, Germany
e-mail: delphine.christin@seemoo.tu-darmstadt.de; matthias.hollick@seemoo.tu-darmstadt.de

S. Gutwirth et al. (eds.), *European Data Protection: Coming of Age*,
DOI 10.1007/978-94-007-5170-5_9,

opt out of the application, thus decreasing the quality of the gathered data. Privacy protection is therefore mandatory to encourage potential contributions.

Within the scope of this manuscript, we investigate the technological basis for mobile sensing applications. We analyze the different sensor modalities collected in existing applications in order to highlight the respective threats to privacy. We further examine how the sensor readings are processed within the architecture of typical mobile sensing applications. We consider the current state-of-the-art in privacy-protection mechanisms. We particularly concentrate on mechanisms applied on either the collected sensor readings or the associated spatiotemporal information. Moreover, we distinguish mechanisms in which the personal privacy conception of the volunteers is taken into account, from mechanisms remaining transparent for the users. Based on the analysis of the current state-of-the-art, we identify and discuss future research directions.

The remaining of the manuscript is organized as follows. In Sect. 9.2, we discuss the benefits of leveraging mobile phones as sensing platform and present selected application scenarios. We analyze the threats to privacy resulting from the collection of the sensor readings in Sect. 9.3 and present selected privacy-preserving mechanisms in Sect. 9.4. We discuss future research directions in Sect. 9.5, before making concluding remarks in Sect. 9.6.

9.2 Mobile Phones as Sensing Platform

In this section, we highlight different factors in favor of the adoption of mobile phones as sensing platforms and illustrate how they can be leveraged by presenting selected existing deployment scenarios.

9.2.1 A Trilogy of Adoption Factors

In the last decades, sensing-oriented applications have mostly been built around dedicated sensing platforms, such as the Sun SPOT[4] or TelosB[5] platforms, or platforms specially tailored to the application requirements. Most of these platforms have been conceived to be deployed unattended for long periods of time. This implies the utilization of batteries as power supply and the limitation of both the size of the platform and its resources. Dedicated sensing nodes offer scarce processing and storage resources that constraint the collection of rich types of sensor readings and the application of complex algorithms. As a result, their deployment remains limited to small scale and static application, and has not yet led to widespread

[4] "Sun SPOT Main Board Technical Datasheet," http://www.sunspotworld.com (accessed in 02.2012).

[5] "TelosB Datasheet," http://www.memsic.com (accessed in 02.2012).

deployment outside highly specialized niche applications. On the contrary, mobile phones benefit from a trilogy of factors in favor of their adoption as sensing platforms, which we detail in the following sections.

9.2.1.1 Technological Factor

Recent mobile phones offer continuously increasing resources, and integrate more and more sensors and wireless technologies. Indeed, mobile phones are equipped with powerful processors and substantial amount of memory.[6] Both cater for complex processing on the device itself and widen the range of possible sensing application scenarios. They also integrate a large number of sensors. For example, the 2011 iPhone 4S[7] features a gyroscope, accelerometers, a digital compass, a proximity sensor, a light sensor, two cameras and two microphones. In comparison, TelosB platforms are equipped with proximity, light, humidity, and temperature sensors. The mobile phone's sensors enable the collection of rich information about the users and their environments. Moreover, the on-board sensors can be easily extended by external sensors interfaced via Bluetooth in order to collect further information. The collected sensor readings can be automatically annotated with the time and location of their collection using integrated positioning systems, such as assisted GPS, digital compass, Wi-Fi, and cellular triangulation. Moreover, mobile phones enable an easy transmission of the collected sensor readings to the application using standard cellular or Wi-Fi-based communication, while dedicated sensing platforms utilize the specific IEEE 802.15.4 standard tailored for their scarce resources.

9.2.1.2 Human Factor

Mobile phones have been already adopted by over five billion users[8] and are part of our daily life. Mobile phones are carried by the population while, e.g., commuting, or practicing leisure activities. This acceptance by the population at large provides for unprecedented coverage and mobility, and opens the doors for novel application scenarios. Mobile phones can capture data about impromptu events, which are not covered by static sensing deployment. They also enable the analysis of relationships between users and their relationships with their environment. Besides, the online marketplaces for apps and their exponentially growing market offer an unprecedented visibility for sensing application. Using these services, the application developers can easily come into contact with millions of people and democratize sensing applications.

---

[6] Delphine Christin and Matthias Hollick, "We Must Move – We Will Move: On Mobile Phones as Sensing Platforms," in *Proceedings of the 10th GI/ITG KuVS Fachgespräch Drahtlose Sensornetze (FGSN)*, 2011.

[7] "iPhone 4S Technical Specifications," http://www.apple.com (accessed in 02.2012).

[8] "Global GSM and 3GSM Mobile Connections," http://www.gsm.com (accessed in 02.2012).

9.2.1.3 Economical Factor

The download of the sensing applications from online marketplaces allows the application developers to exploit already deployed mobile phones. This reduces the deployment costs to virtually zero. In comparison, existing wireless sensor networks require specific hardware, whose costs are supported by the application developers and later, by the application operators.

9.2.2 Selected Application Scenarios

The combination of the above factors has lead to the emergence of a plethora of mobile sensing applications making use of mobile phones in recent years. These applications investigate manifold subjects of study, ranging from the automated collection of petrol prices by means of pictures taken by the mobile phones mounted on the passenger seat in cars[9] to the calculation of the environmental impact and the exposure to particles of users.[10] In order to illustrate the variety of the possible application scenarios, we have selected three application scenarios and provide herein details about their deployments.

9.2.2.1 Sport Performances

Current mobile phones can be used to monitor and document the performances of users while practicing physical activities. For example, the BikeNet[11] and the *Biketastic*[12] projects provide information about the users' experiences while bicycling. The location information provided by the positioning system (GPS or GSM radio) are completed by sensor readings collected using both embedded and peripheral sensors wirelessly connected to the mobile phones. The combination of these data enables to draw a fine-grained portrait of the cyclist's performances, including speed, burnt calories, or galvanic skin response.

9.2.2.2 Road Conditions

Mobile phones can also be utilized to monitor road conditions and detect traffic congestion.[13] The embedded accelerometers provide indications on the surface

[9] Yi F. Dong et al., "Automatic Collection of Fuel Prices from a Network of Mobile Cameras," in *Proceedings of the 4th IEEE International Conference on Distributed Computing in Sensor Systems (DCOSS)*, 2008.

[10] Min Mun et al., "PEIR, the Personal Environmental Impact Report, as a Platform for Participatory Sensing Systems Research," in *Proceedings of the 7th ACM International Conference on Mobile Systems, Applications, and Services (MobiSys)*, 2009.

[11] Shane B. Eisenman et al., "BikeNet: A Mobile Sensing System for Cyclist Experience Mapping," *ACM Transactions on Sensor Networks* 6 (2009).

[12] Shilton, "Four Billion Little Brothers?".

[13] Mohan, "Nericell".

roughness of the roads by detecting potholes and bumps, while the microphones monitor braking and honking in order to detect potential traffic congestion. The collected sensor readings are annotated with spatiotemporal information and transmitted to the application to build maps available to the public.

9.2.2.3 Noise Pollution

Mobiles phones can provide insights about noise pollution in urban environment as proposed in, e.g., the *Ear-Phone*,[14] *NoiseSpy*,[15] and *NoiseTube*[16] applications. The embedded microphones collect sound samples, which are directly processed on the mobile phone to extract the corresponding loudness level. The results are then transmitted to the application, which consolidates noise pollution maps. These maps can be consulted by the public or specialists investigating relationships between noise exposition and human behavioral problems.

In summary, the data gathered by the mobile phones cannot only benefit to the participants in mobile sensing applications themselves, but also to the community.

9.3 On the Need of Privacy-Protection Mechanisms

We identify potential threats to the privacy of the contributing users by first considering the sensor readings collected. Next, we discuss the privacy implications connected with their processing in the typical architecture of current mobile sensing applications.

9.3.1 Privacy-Sensitive Sensor Readings and Spatiotemporal Annotations

We concentrate on the following primary information/sensor readings collected in most of existing mobile sensing deployments[17] and highlight the corresponding potential threats to privacy: (1) spatiotemporal information, (2) sound samples, (3) pictures and videos, and (4) accelerometer data.

---

[14] Rana, "Ear-Phone".

[15] Eiman Kanjo et al., "MobSens: Making Smart Phones Smarter," *IEEE Pervasive Computing* 8 (2009).

[16] Nicolas Maisonneuve et al., "NoiseTube: Measuring and Mapping Noise Pollution with Mobile Phones," in *Proceedings of the 4th International Symposium on Information Technologies in Environmental Engineering (ITEE)*, 2009.

[17] Delphine Christin et al., A Survey on Privacy in Mobile Participatory Sensing Applications, *Journal of Systems & Software* 84 (2011).

9.3.1.1 Spatiotemporal Information

With a few exceptions, most of current mobile sensing applications collect location information about the users.[18] The location information can either be directly used by the application or serve to annotate the collected sensor readings in space and time. The precision of the location information depends on the utilized positioning system. GPS receivers provide accurate coordinates; while WiFi or cellular network based triangulation provide coarse-grained location information.[19] Moreover, the location of users can also be inferred from collected sound samples, which reveal the noise surrounding the users. The collected and/or inferred location information poses a risk for the privacy of the users since it may leak personal information, such as routines or habits of the users.[20] For example, the medical conditions of users may be inferred from frequent visits to hospitals or political views from attendances at political events.[21] Even if users contribute anonymously to the application using e.g., pseudonyms, their identity may be inferred based on an analysis of their commute patterns, which easily reveals domicile and workplace locations. A simple reverse white page lookup is sufficient to de-anonymize most anonymous users.[22] This information may also be made available by the mobile operator to the application developers or managers. Furthermore, temporal annotations of sensor data can provide insights about the habits of the users and hence, endanger their privacy. While spatiotemporal information already threaten the privacy of the users in their own, the threats to privacy further increase when these information are combined with the following sensor modalities.

9.3.1.2 Sound Samples

Current mobile sensing applications record sound samples in order to, e.g., measure surrounding noise level.[23] The recording process is either automated or initiated by the users. In the automated procedure, this recording poses serious risks for the user privacy in absence of privacy-preserving mechanisms, since confidential and intimate conversations may be recorded. In the assisted procedure, the users can directly assess potential threats to privacy and intentionally decide to start the recording. Sound samples may not only record personal conversations, but may also reveal sensitive information about the user's current context and thus, his possible location.

---

[18] Christin, A Survey on Privacy in Mobile Participatory Sensing Applications.

[19] Anthony LaMarca et al., "Place Lab: Device Positioning Using Radio Beacons in the Wild," *Pervasive Computing* 3468 (2005).

[20] Shilton, "Four Billion Little Brothers?".

[21] Ling Liu, "From Data Privacy to Location Privacy: Models and Algorithms," in *Proceedings of the 33rd International Conference on Very Large Data Bases (VLBD)*, 2007.

[22] John Krumm, "Inference Attacks on Location Tracks," in *Proceedings of the 5th IEEE International Conference on Pervasive Computing (Pervasive)*, 2007.

[23] Rana, "Ear-Phone".

9.3.1.3 Pictures and Videos

Few mobile sensing applications make use of pictures and videos to document the events of interest.[24] Similarly to the collection of sound samples, the collection of pictures and videos can be either automated or assisted. Most of existing applications however rely on pictures intentionally taken by the users.[25] This assisted process not only enables the users to directly protect their privacy, but also increases the relevance and quality of the pictures and videos. Pictures and videos can however endanger the privacy of additional people captured in the images by the users. This may reveal their current locations as well as the identity of their social relations.

9.3.1.4 Acceleration

Accelerometer data are collected to provide information about, e.g., the roughness of the streets.[26] Compared to the aforementioned sensor modalities, they may appear to be less threatening to the privacy of the users. However, it has been shown that a mobile phone carried on the hip of a user and recording his acceleration allows to identify characteristics of his gait, which may lead to the inference of his identity.[27] Moreover, personal information, such as passwords entered or emails sent on nearby keyboards, can be revealed by an analysis of the accelerometer data collected on-board.[28]

In summary, in absence of privacy-preserving mechanisms, the collected sensor readings may reveal diverse personal and sensitive information about the contributing users, ranging from their whereabouts to their social contacts or environment. Mechanisms are thus required to prevent the inference of personal information from the collected sensor readings and hence, protect the privacy of the contributing users. Note that future mobile sensing applications may be extended to further sensor modalities, such as using stylus or touch screens or wireless interfaces (e.g., NFC, Wi-Fi, or Bluetooth) for capturing personal information about the users and other users in their surroundings. The capture of this information raises new threats to privacy. However, we consider the analysis of these additional modalities as out of scope of this manuscript.

---

[24] Christin, A Survey on Privacy in Mobile Participatory Sensing Applications.

[25] Ibid.

[26] Mohan, "Nericell".

[27] Mohammad O. Derawi et al., "Unobtrusive User-authentication on Mobile Phones using Biometric Gait," in *Proceeding of the 6th IEEE International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP)*, 2010.

[28] Philip Marquardt et al., "(sp)iPhone: Decoding Vibrations from Nearby Keyboards using Mobile Phone Accelerometers," in *Proceedings of the 18th ACM Conference on Computer and Communications Security (CCS)*, 2011.

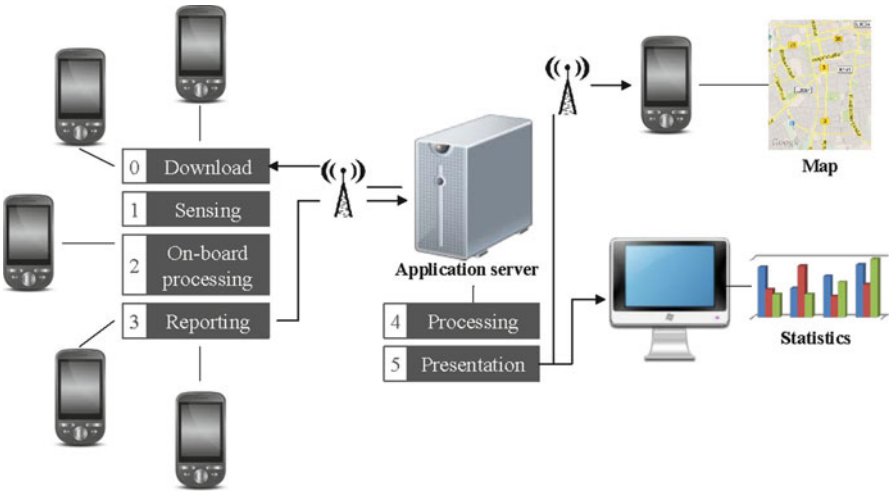


Fig. 9.1 Architecture overview

9.3.2 Centralized Architecture

We present a common architectural model of existing mobile sensing applications and detail the different stakeholders and information flows involved. As illustrated in Fig. 9.1, most architectures are organized in a centralized fashion, where mobile phones interact with an application server. We assume that users first download the application on their mobile phones from, e.g., an online marketplace or the website of the application. The downloaded application is already configured to collect the sensor readings. Depending on the nature of the application, users may be involved in the collection process and need to intentionally start/stop this process. Once the sensor readings are collected, they may directly be processed on the mobile phones. This on-board processing enables to, e.g., extract features of interest, such as the sound level of audio samples,[29] or display the sensor readings directly on the mobile phone of the contributing user in an appropriate form, such as maps and diagrams.[30] The sensor readings are then wirelessly transmitted to the application server managed by the application developers. The application developers are involved in the design, the implementation, and the deployment of the application and its infrastructure. The transfer of the sensor readings to the application server mostly relies on standard communication infrastructures, such as Wi-Fi, or GSM/GPRS/3G connectivity. The transferred sensor readings are then processed at large scale on the application server in order to, e.g., compute summaries over all contributing users or prepare

[29] Rana, "Ear-Phone".

[30] Bret Hull et al., "CarTel: A Distributed Mobile Sensor Computing System," in *Proceedings of the 4th ACM International Conference on Embedded Networked Sensor Systems (SenSys)*, 2006.

their presentation to end users. The processed results are finally displayed to the end users in forms of graphs, maps, or geographic overlays. They can also be presented as raw data in order to allow end users to analyze the sensor readings themselves. End users include, e.g., users contributing to the application willing to consult their own sensor readings or compare them with others, specialists willing to analyze particular phenomena based on the collected sensor readings, or the general public.

In summary, the sensor readings collected by the contributing users are first accessed by the application developers and later, by the end users. Contributing users need thus to first trust the application developers not to disclose their sensor readings to unauthorized third parties and secondly, to apply efficient mechanisms to protect their privacy when the sensor readings are released to the end users.

9.4 State-of-the-Art in Privacy Protection

As highlighted above, mobile sensing applications require the application of privacy-preserving mechanisms due to the collection and processing of privacy-sensitive sensor readings. In the following, we study the current state-of-the-art of privacy-preserving mechanisms specially geared towards mobile sensing applications. We have classified these mechanisms into two categories: user-controlled and application-controlled mechanisms, based on the degree of involvement of the users in the privacy decisions.

9.4.1 User-Controlled Privacy-Preserving Mechanisms

In this section, we present selected mechanisms in which the users are involved in the control of their privacy. This includes the utilization of pseudonyms, the selection of the sensor readings to release and the users authorized to access them, as well as the personal management of the sensor readings' storage.

9.4.1.1 Utilization of Pseudonyms

Users contributing to mobile sensing applications can decide to use an alias to register to the application and report sensor readings. By doing so, users believe that they do not reveal their real identity to the application. However, the spatiotemporal annotations of the transmitted sensor readings may reveal this information, despite the use of pseudonyms. In fact, the annotations may show the commuting pattern of the users between their domicile and workplace locations. The utilization of reverse address lookups enables to retrieve the names of the users living in the identified locations.[31] Consequently, the supposed anonymity provided by the use of pseudonyms becomes void as soon as fine-grained location information is provided to the application.

[31] Krumm, "Inference Attacks on Location Tracks".

9.4.1.2 Selection of Sensor Readings

Another measure to protect privacy consists in disabling the sensing function when users feel that their privacy is endangered.[32] While this measure efficiently protects the privacy of the users, it simultaneously endangers the viability of the application, since no sensor readings are reported. Instead of disabling the sensing function, users can also control the degree of granularity at which their sensor readings are released to the application.[33] For example, users may choose to release only the name of the streets in which the sensor readings were collected instead of the exact coordinates. In this case, the privacy of the users can be preserved if the selected degree of granularity is sufficiently coarse to remove privacy-sensitive information. Simultaneously, the application can benefit from some insights provided by the reported sensor readings, even if they are not fine-grained. This solution hence proposes a balanced tradeoff between the needs of the application and the protection of the users' privacy. Users can set additional parameters to refine the selection of the sensor readings they are willing to release. For example, they can choose particular data types and define spatiotemporal conditions under which the data are made accessible.[34] Additionally, users can select sensitive locations, which are then protected using location selective hiding.[35] When users approach a location they have previously defined as sensitive, the application running on their mobile phone computes a fictitious location trace, which does not include the sensitive location. The new computed trace takes into consideration the mapping of nearby streets and the history of the users in order to improve the realism of the new trace. Moreover, the sensor readings collected during this period are adapted to the new trace's characteristics in order to maintain the consistency of the application results.

9.4.1.3 Selection of Authorized Users

In addition to the selection of the sensor readings to release, the users can determine which categories of users are authorized to access them. For example, the users can decide to confine the data to their own use. In this case, the application developers who manage the application infrastructure would still have access to the sensor readings as soon as they are transferred to the application server. The users can also share their sensor readings with individuals, groups, or make them available to the public.

---

[32] Katie Shilton et al., "Participatory Privacy in Urban Sensing," in *Proceedings of the International Workshop on Mobile Devices and Urban Sensing (MODUS)*, 2008.

[33] Tathagata Das et al., "PRISM: Platform for Remote Sensing using Smartphones," in *Proceedings of the 8th ACM International Conference on Mobile Systems, Applications, and Services (MobiSys)*, 2010.

[34] Shilton, "Participatory Privacy in Urban Sensing".

[35] Mun, "PEIR".

9.4.1.4 User-Controlled Storage

In both the selection of the sensor readings and authorized users, the users must trust the application to apply the correct access control rules and not disclose the sensor readings to unauthorized users or at finer degree of granularities. In order not to rely on the application, the users can make use of *virtual individual servers*[36] and control the release of their information themselves. The users upload their raw data on these personal virtual machines and individually configure their access to the different applications they are registered in. This solution allows the users to maintain a control over their data and dynamically adapt both the authorized users and sets of data according to their personal privacy preferences.

9.4.2 Application-Controlled Privacy-Preserving Mechanisms

Contrary to the aforementioned mechanisms, the mechanisms presented in this section remain transparent for the users and do not involve them in any privacy decision. We specially focus on mechanisms applied on sensor readings and location information provided to the application.

9.4.2.1 Perturbation of Sensor Readings

The perturbation of sensor readings, i.e., the process of removing privacy-sensitive information from the sensor readings, can happen either on the mobile phone or on the application server. In the following, we first consider on-board processing before addressing potential processing on the application server. Depending on the application, algorithms can run on the mobile phone to directly extract the features of interest from the raw sensor readings without requiring their transfer to the application server. For example, the Ear-Phone application[37] determines the loudness level of the collected sound samples directly on the mobile phones, and only transfers this information to the application. Additional classifiers can be applied to, e.g., detect and eventually eliminate human voices recorded in the sound samples.[38] This privacy-aware processing may thus eliminate privacy-sensitive elements contained in the sensor readings at the source. The spectrum of the applied algorithms is however

[36] Ramón Cáceres et al., "Virtual Individual Servers as Privacy-Preserving Proxies for Mobile Devices," in *Proceedings of the 1st ACM Workshop on Networking, Systems, and Applications for Mobile Handhelds (MobiHeld)*, 2009.

[37] Rana, "Ear-Phone".

[38] Emiliano Miluzzo et al., "Sensing Meets Mobile Social Networks: The Design, Implementation and Evaluation of the CenceMe Application," in *Proceedings of the 6th ACM Conference on Embedded Network Sensor Systems (SenSys)*, 2008.

limited by the resources of the mobile phones, which are still scarcer compared to those offered by personal computers. Instead of extracting features of interest, artificial noise can also be intentionally added to the sensor readings before their transfer to the application server. The added noise perturbs the individual sensor readings in such a way that their individual characteristics cannot be recognized anymore, but the computation of trends and distribution at a community scale is still possible.[39] Additional perturbation can be applied on the server side. For example, the application developers can remove the identity associated to the sensor readings or any specificities of the sensor readings susceptible to lead to the identification of the corresponding user. They can also aggregate the sensor readings obtained by several participants in forms of statistics or maps in order to diminish the degree of granularity of the disclosed information. Note that in both cases, the application developers have access to the individual sensor readings. If the sensor readings have not been priorily perturbed on the mobile phones, this may seriously endanger the privacy of the users in case of malicious application developers.

9.4.2.2 Perturbation of Location Information

The exact location of the collection of the sensor readings can also be intentionally perturbed to protect the location privacy of the participants. The primary idea behind the perturbation is to build groups of k users who share a common attribute, rendering the users indistinguishable from each other according to the principle of k-anonymity.[40] For example, k users located in the same district form such a group. Different methods have been proposed to find a common attribute for the users and build groups of at least k of them. One method, called *tessellation*, generalizes the exact location of the users by a location with less degree of detail.[41] For this purpose, the related geographic area is divided into multiple tiles, each of them containing at least k users. Instead of the exact coordinates of their collection, the sensor readings are annotated using the geographical boundaries or center of the current tile.[42] Since the k users included in the same tile annotate their sensor readings with the same information, they become indistinguishable. Another method called *microaggregation* replaces the exact coordinates of the users by the average location of the k nearest users and similarly protects the location privacy of the k users.[43] While both methods

[39] Raghu K. Ganti et al., "PoolView: Stream Privacy for Grassroots Participatory Sensing," in *Proceedings of the 6th ACM Conference on Embedded Network Sensor Systems (SenSys)*, 2008.

[40] Latanya Sweeney, "K-Anonymity: A Model for Protecting Privacy," *International Journal of Uncertainty, Fuzziness, and Knowledge-Based Systems* 10 (2002).

[41] Minho Shin et al., "AnonySense: A System for Anonymous Opportunistic Sensing," *Journal of Pervasive and Mobile Computing* 7 (2010).

[42] Kuan L. Huang, Salil S. Kanhere, and Wen Hu, "Preserving Privacy in Participatory Sensing Systems," *Computer Communications* 33 (2010).

[43] Josep Domingo-Ferrer and Josep M. Mateo-Sanz, "Practical Data-Oriented Microaggregation for Statistical Disclosure Control," *IEEE Transactions on Knowledge and Data Engineering* 14 (2002).

prevent from distinguishing the k users included into each group, they however still require the communication of the exact coordinates to a central entity for the calculation of the tiles or the averaged location. If this central entity cannot be trusted, the privacy of the users is again in danger.

Additional mechanisms can also be applied to protect the anonymity and privacy of the users while interacting with the infrastructure.[44] They however remain out of scope of this manuscript, which focuses on the privacy threats resulting from the gathering of sensor readings.

9.5 Future Directions

Above, we have outlined the threats to privacy resulting from the collection of spatiotemporally annotated sensor readings in mobile sensing applications. We have also presented selected existing mechanisms to protect the privacy of the contributing users and highlighted related issues. In this section, we propose future directions for the protection of privacy in mobile sensing applications. Note that our list of future directions is by no means exhaustive, but includes our view on the most relevant challenges at the time of writing this article.

9.5.1 Integration of Privacy-Preserving Solutions

The combination of the privacy-preserving mechanisms discussed in Sect. 9.4 gives the impression that they cater for a complete solution, which efficiently ensures the privacy protection of the users. However, most of them have been proposed in different work and have not been integrated into a sole mobile sensing application. Moreover, a study of more than 30 existing mobile sensing applications have shown that only few of them integrate privacy-preserving mechanisms in their original design.[45] This particularly highlights the lack of synergy between application developers and developers of privacy-preserving solutions, who generally belong to two different communities. While application developers often consider privacy-protecting features as important, they reserve their integration into the application for later development stages.[46] However, integrating privacy-preserving mechanisms into existing applications may be more complex than their integration during the design of the application itself. As a result, it may happen that this integration never happens in the worst case. The lack of privacy protection may limit the contribution of

[44] Christin, A Survey on Privacy in Mobile Participatory Sensing Applications.

[45] Ibid.

[46] Marc Langheinrich, "Personal Privacy in Ubiquitous Computing – Tools and System Support" (Ph.D. diss., ETH Zurich, 2005).

potential users and seriously endanger the viability of the application. We therefore believe that the synergy between both communities of application developers and privacy specialists should be improved to protect the privacy of the contributing users and propose enhanced privacy-protection solutions specially tailored to the real needs of the targeted applications.

9.5.2 Decentralized Mechanisms

As illustrated in Sect. 9.4.2, users of mobile sensing applications must rely on the application not to disclose their sensor readings to unauthorized third parties. Indeed, once the sensor readings are uploaded on the application server, the users lose the control over their data. While they can configure different settings concerning the data release, they have no guarantees that their preferences are respected by the application. The personal virtual machines detailed in Sect. 9.4.1.4 count among the first methods to give the control over their data back to users. Additional methods have been proposed in which, e.g., users autonomously protect their privacy by physically exchanging their sensor readings with other users.[47] The exchange unlinks the identity of the users from sensor readings they have collected. As a result, the location visited by the users is no more directly linked to their identity. We believe that additional efforts are required in this direction in order to reduce the dependence of the users on the application developers while still supporting their contributions to the application. These next steps will however require a careful analysis of possible solutions, since giving more control to the users inherently introduces additional overheads for the users. These overheads should be limited to the minimum in order to encourage their acceptance and utilization by potential users.

9.5.3 Involvement of the Users

Different mechanisms directly involve the users in the privacy decisions as highlighted in Sect. 9.4.1. This approach is important to allow the users to configure the privacy settings of the application according to their privacy preferences and reflect their personal privacy conception. However, most of them have not been evaluated by means of user studies, meaning that their usability has not been analyzed yet. For example, no hints have been provided for the realization of the selection of the different degrees of granularity at which the sensor should be released[48] or no evaluation of the personal virtual machines (see Sect. 9.4.1.4) indicates their acceptance by potential users. To address this issue, we believe that the development of

[47] Delphine Christin et al., "Privacy-Preserving Collaborative Path Hiding for Participatory Sensing Applications," in *Proceedings of the 8th IEEE International Conference on Mobile Ad-hoc and Sensor Systems (MASS)*, 2011.

[48] Das, "PRISM".

every user-centered privacy-preserving mechanisms should involve potential users. Indeed, research results from orthogonal domains have demonstrated that not considering the users mostly leads to either an inefficient application of the mechanisms supposed to protect the users or even their non-utilization by the users. For example, it was demonstrated that most users keep written copies of their passwords and thus reduce the efficacy of password-based authentication mechanisms.[49] Moreover, most users do not protect their email transmission due to the complexity of the involved security mechanisms.[50] In order to avoid these pitfalls, we propose therefore the following steps for the development of new user-controlled mechanisms.

9.5.3.1 Requirements Analysis

A preliminary study should be conducted by interviewing potential users in order to determine their real needs and also identified related requirements. These interviews should explore different dimensions of the proposed design. For example, users could provide indications about how much time they would be ready to invest to personalize the privacy settings or utilize the mechanism, which information are essential to understand the consequences of their choices, in which form should they be represented, etc. The goals of such interviews should be to, e.g., sort out superfluous from crucial information, and identify the maximal overhead accepted by the participants. Moreover, the interviews should enable to determine whether the proposed mechanism can be presented in a fashion, which is understandable for all, and if possible, how it should be done.

9.5.3.2 Development of User-Friendly Solutions

Based on the results of the first interviews, the design of the proposed solution should be refined and adapted to the identified needs and requirements of the users. This may include the development of user interfaces making the proposed solution visible to the users. In this stage, particular attention should be paid to the usability of the proposed solution, including its ease of use, its ease of comprehend, etc. Multiple solutions can be developed to later explore the preferences of the users.

9.5.3.3 Evaluation of the Developed Solutions

Once the solutions have been designed and implemented, they should be evaluated by potential users using firstly a short-term user study. The feedbacks of the users

[49] Anne Adams and Martina A. Sasse, "Users Are Not the Enemy". *Communications of the ACM* 42 (1999).

[50] Alma Whitten and J. D. Tygar, "Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0," in *Proceedings of the USENIX Security Symposium (SSYM)*, 1999.

should be taken into consideration to still improve the design of the proposed solutions. Secondly, a long-term user study should be conducted to investigate the solutions over longer period of time and tested them under real-world conditions. The results of this study should be used to refine the proposed solutions until reaching its final version.

While including potential users in the loop for the design of new solutions may appear cumbersome and resource-consuming, we believe that the additional overheads would be compensated by an increased acceptance of the proposed mechanisms and consequently, an enhanced privacy protection. Conducting such studies may however be difficult, as most applications are still in their infancy and have not been accepted at large scale. Finding users actively contributing to these applications may thus be demanding. By default, the spectrum of possible participants of such studies can be extended to common users of smartphones, since most of them are used to install various applications from online marketplaces on their devices and hence, have a certain experience in interacting with them.

In summary, providing privacy solutions for mobile sensing applications is not only about fulfilling technical requirements, but also about considering human requirements especially by means of, e.g., interaction design.

9.5.4 Privacy Awareness

In recent years, the awareness of users about potential privacy threats resulting from the utilization of mobile applications has incrementally raised. However, it still does not reach the same degree of awareness as in other domains, such as the recording of license plates on cars and the utilization of CCTV camera by the police. Surveillance by the governmental entities is often perceived as threat to the privacy of the citizens, while mobile applications may appear inoffensive since they are not controlled by central and official bodies. However, the development of new applications is open to anybody and the control over these application is limited to the verifications conducted by the marketplaces before the application's release. This may seriously endanger the privacy of the users if inappropriate information is collected about them. Innovative methods need still to be invented to efficiently increase the awareness of the users about these particular privacy issues. Existing solutions, such as textual warnings, may be insufficient to fulfill this goal, since they are often discarded by the users without having been read. New methods catering for an easy visualization of the existing threats including, e.g., dedicated color mapping or symbols, need to be investigated. Furthermore, this would also require the introduction of independent and trusted third parties, which would be responsible for auditing and evaluating the risks for the user's privacy for each application. Otherwise, malicious application developers may underestimate the privacy threats of their own application to favor their utilization by potential users. The feasibility and later the integration of such parties into the current ecosystem need therefore to be carefully studied.

9.5.5 Identity Management

Existing privacy-aware solutions tailored to the requirements of mobile sensing applications often consider the identity and the location of the users as two distinct kinds of information to protect. In domains orthogonal to mobile sensing such as location-based services, location is, however, seen as part of the user's identity.[51] By including additional information captured by onboard sensors, the concept of digital identity introduced in these domains could be extended and applied in mobile sensing applications. As a result, privacy-preserving mechanisms inspired by existing solutions developed for e.g., location-based services[52] could be tailored to the specific requirements of mobile sensing applications. This would allow to investigate new research questions related to identity management in mobile sensing and refine the definition of identity by including further privacy-relevant information, such as sensor data collected using mobile phones.

9.5.6 Adoption, Utilization, and Privacy

While several privacy-preserving mechanisms have been developed in the recent years for mobile sensing applications, only little attention has been paid to the influence of the degree of privacy protection on the adoption of the applications by the users. Similar to studies conducted in orthogonal domains, such as online banking,[53] the importance of privacy as an adoption factor should be investigated in order to better understand the fears of potential users. In response, adapted privacy-preserving solutions could be proposed in order to increase the acceptance of the applications by potential users. Another aspect to investigate is how users make use of these solutions in the field, e.g., if they change their privacy settings, how they change them, or which are the working solutions and parameter sets. Outcomes of such studies could allow to refine the design of the proposed solutions and tailor them to the real needs of users having tested them under real-world conditions.

---

[51] Lothar Fritsch, "Profiling and Locations-Based Services", in *Profiling the European Citizen – Cross-Disciplinary Perspective*, ed. Mireille Hildebrandt and Serge Gutwirth (Dordrecht: Springer Netherlands), 2008.

[52] Jan Zibuschka et al., "Enabling Privacy of Real-Life LBS: A Platform for Flexible Mobile Service Provisioning," in *Proceedings of the 22nd IFIP TC-11 International Information Security Conference*, 2007.

[53] Ming-Chi Lee, "Factors Influencing the Adoption of Internet Banking: An Integration of TAM and TPB with Perceived Risk and Perceived Benefit," *Electronic Commerce Research and Applications* 8 (2009).

9.6 Conclusions

Mobile sensing applications promise improvement in the everyday life of citizens. However, at the same time, they pose a threat to citizens' privacy. We have first detailed the trilogy of factors in favor of the adoption of mobile phones as sensing platforms and presented selected application scenarios in order to highlight potential benefits drawn from their utilization. We have then studied the different information collected by existing mobile sensing applications and the information flow within the supporting application architectures. We have particularly emphasized on the threats to privacy resulting from the collection of this information as well as on the information processing. In a next step, we have discussed selected privacy-preserving mechanisms. In particular, we have considered the parameters controlled by the users, which allows them to directly configure the settings of the mechanisms according to their privacy preferences and those which remain transparent to the users and are primarily managed by the application. Based on these discussions, we have identified different future research directions in which additional efforts should be provided in long-term. We consider these fields of research as of particular interest for the European privacy community, which can build on extensive related work in the area of location based services or vehicular communications. Mobile sensing applications are about to cross the chasm to mass deployment, yet the research landscape in this application domain is fragmented and many open challenges persist. Addressing these challenges would benefit both the research community as well as the European citizens and society at large.

References

Adams, Anne, and Martina A. Sasse. 1999. Users are not the enemy. *Communications of the ACM* 42: 40–46.

Cáceres, Ramón, Landon Cox, Harold Lim, Amre Shakimov, and Alexander Varshavsky. 2009. Virtual individual servers as privacy-preserving proxies for mobile devices. In *Proceedings of the 1st ACM workshop on networking, systems, and applications for mobile handhelds (MobiHeld)*, 37–42, Barcelona, Spain.

Christin, Delphine, and Matthias Hollick. 2011. We must move – We will move: On mobile phones as sensing platforms. In *Proceedings of the 10th GI/ITG KuVS Fachgespräch Drahtlose Sensornetze (FGSN)*, 25–28, Paderborn, Germany.

Christin, Delphine, Andreas Reinhardt, Salil S. Kanhere, and Matthias Hollick. 2011a. A survey on privacy in mobile participatory sensing applications. *Journal of Systems and Software* 84: 1928–1946.

Christin, Delphine, Julien Guillemet, Andreas Reinhardt, Matthias Hollick, and Salil S. Kanhere. 2011b. Privacy-preserving collaborative path hiding for participatory sensing applications. In *Proceedings of the 8th IEEE international conference on mobile ad-hoc and sensor systems (MASS)*, 341–350, Valencia, Spain.

Das, Tathagata, Prashant Mohan, Venkat Padmanabhan, Ramachandran Ramjee, and Asankhaya Sharma. 2010. PRISM: Platform for remote sensing using smartphones. In *Proceedings of the 8th ACM international conference on mobile systems, applications, and services (MobiSys)*, 63–76, San Francisco, California, USA.

Derawi, Mohammad O., Claudia Nickel, Patrick Bours, and Christoph Busch. 2010. Unobtrusive user-authentication on mobile phones using biometric gait. In *Proceeding of the 6th IEEE international conference on intelligent information hiding and multimedia signal processing (IIH-MSP)*, 306–311, Darmstadt, Germany.

Domingo-Ferrer, Josep, and Josep M. Mateo-Sanz. 2002. Practical data-oriented microaggregation for statistical disclosure control. *IEEE Transactions on Knowledge and Data Engineering* 14: 189–201.

Dong, Yi F., Salil S. Kanhere, Chun T. Chou, and Nirupama Bulusu. 2008. Automatic collection of fuel prices from a network of mobile cameras. In *Proceedings of the 4th IEEE international conference on distributed computing in sensor systems (DCOSS)*, 140–156, Santorini Island, Greece.

Eisenman, Shane B., Emiliano Miluzzo, Nicholas D. Lane, Ronald A. Peterson, Gahng-Seop Ahn, and Andrew T. Campbell. 2009. BikeNet: A mobile sensing system for cyclist experience mapping. *ACM Transactions on Sensor Networks* 6: 1–39.

Fritsch, Lothar. 2008. Profiling and location-based services. In *Profiling the European citizen – Cross-disciplinary perspectives*, ed. Mireille Hildebrandt and Serge Gutwirth, 147–160. Dordrecht: Springer.

Ganti, Raghu K., Nam Pham, Yu-En Tsai, and Tarek F. Abdelzaher. 2008. PoolView: Stream privacy for grassroots participatory sensing. In *Proceedings of the 6th ACM conference on embedded network sensor systems (SenSys)*, 281–294, Raleigh, NC, USA.

Huang, Kuan L., Salil S. Kanhere, and Hu Wen. 2010. Preserving privacy in participatory sensing systems. *Computer Communications* 33: 1266–1280.

Hull, Bret, Vladimir Bychkovsky, Yang Zhang, Kevin Chen, Michel Goraczko, Allen Miu, Eugene Shih, Hari Balakrishnan, and Samuel Madden. 2006. CarTel: A distributed mobile sensor computing system. In *Proceedings of the 4th ACM international conference on embedded networked sensor systems (SenSys)*, 125–138, Boulder, Colorado, USA.

Kanjo, Eiman, Jean Bacon, Peter Landschoff, and David Roberts. 2009. MobSens: Making smart phones smarter. *IEEE Pervasive Computing* 8: 50–57.

Krumm, John. 2007. Inference attacks on location tracks. In *Proceedings of the 5th IEEE international conference on pervasive computing (Pervasive)*, 127–143, Toronto, Canada.

LaMarca, Anthony, Yatin Chawathe, Sunny Consolvo, Jeffrey Hightower, Ian Smith, James Scott, Tim Sohn, James Howard, Jeff Hughes, Fred Potter, Jason Tabert, Pauline Powledge, Gaetano Borriello, and Bill Schilit. 2005. Place lab: Device positioning using radio beacons in the wild. *Pervasive Computing* 3468: 116–133.

Langheinrich, Marc. 2005. Personal privacy in ubiquitous computing – Tools and system support. PhD dissertation, ETH Zurich, Zurich.

Lee, Ming-Chi. 2009. Factors influencing the adoption of internet banking: An integration of TAM and TPB with perceived risk and perceived benefit. *Electronic Commerce Research and Applications* 8: 130–141.

Liu, Ling. 2007. From data privacy to location privacy: Models and algorithms. In *Proceedings of the 33rd international conference on very large data bases (VLBD)*, 1429–1430, Vienna, Austria.

Maisonneuve, Nicolas, Matthias Stevens, Maria E. Niessen, and Luc Steels. 2009. NoiseTube: Measuring and mapping noise pollution with mobile phones. In *Proceedings of the 4th international symposium on information technologies in environmental engineering (ITEE)*, 215–228, Thessaloniki, Greece.

Marquardt, Philip, Arunabh Verma, Henry Carter, and Patrick Traynor. 2011. (sp)iPhone: Decoding vibrations from nearby keyboards using mobile phone accelerometers. In *Proceedings of the 18th ACM conference on computer and communications security (CCS)*, 551–562, Chicago, Illinois, USA.

Miluzzo, Emiliano, Nicholas D. Lane, Kristóf Fodor, Ronald Peterson, Hong Lu, Mirco Musolesi, Shane B. Eisenman, Xiao Zheng, and Andrew T. Campbell. 2008. Sensing meets mobile social networks: The design, implementation and evaluation of the CenceMe application. In *Proceedings of the 6th ACM con embedded network sensor systems (SenSys)*, 337–350, Raleigh, NC, Carolina.

Mohan, Prashanth, Venkata N. Padmanabhan, and Ramachandran Ramjee. 2008. Nericell: Rich monitoring of road and traffic conditions using mobile smartphones. In *Proceedings of the 6th ACM conference on embedded network sensor systems (SenSys)*, 323–336, Raleigh, NC, Carolina.

Mun, Min, Sasank Reddy, Katie Shilton, Nathan Yau, and Jeff Burke. 2009. PEIR, the personal environmental impact report, as a platform for participatory sensing systems research. In *Proceedings of the 7th ACM international conference on mobile systems, applications, and services (MobiSys)*, 55–68, Kraków, Poland.

Rana, Rajib K., Chun T. Chou, Salil S. Kanhere, Nirupama Bulusu, and Wen Hu. 2010. Ear-Phone: An end-to-end participatory urban noise mapping system. In *Proceedings of the 9th ACM/IEEE international conference on information processing in sensor networks (IPSN)*, 105–116, Stockholm, Sweden.

Shilton, Katie. 2009. Four billion little brothers?: Privacy, mobile phones, and ubiquitous data collection. *Communications of the ACM* 52: 48–53.

Shilton, Katie, Jeff Burke, Deborah Estrin, Mark Hansen, and Mani B. Srivastava. 2008. Participatory privacy in urban sensing. In *Proceedings of the international workshop on mobile devices and urban sensing (MODUS)*, 1–7, St. Louis, Missouri, USA.

Shin, Minho, Cory Cornelius, Dan Peebles, Apu Kapadia, David Kotz, and Nikos Triandopoulos. 2010. AnonySense: A system for anonymous opportunistic sensing. *Journal of Pervasive and Mobile Computing* 7: 16–30.

Sweeney, Latanya. 2002. K-anonymity: A model for protecting privacy. *International Journal of Uncertainty, Fuzziness, and Knowledge-Based Systems* 10: 557–570.

Whitten, Alma, and J. D. Tygar. 1999. Why Johnny can't Encrypt: A usability evaluation of PGP 5.0. In *Proceedings of the 8th USENIX security symposium (SSYM)*, 14–29, Washington, DC, USA.

Zibuschka, Jan, Lothar Fritsch, Mike Radmacher, Tobias Scherner, and Kai Rannenberg. 2007. Enabling privacy of real-life LBS: A platform for flexible mobile service provisioning. In *Proceedings of the 22nd IFIP TC-11 international information security conference* (*SEC*), 325–336, Sandton, South Africa.

Global GSM and 3GSM Mobile Connections. http://www.gsm.com. Accessed Feb 2012.

iPhone 4S Technical Specifications. http://www.apple.com. Accessed Feb 2012.

Sun SPOT Main Board Technical Datasheet. http://www.sunspotworld.com. Accessed Feb 2012.

TelosB Datasheet. http://www.memsic.com. Accessed Feb 2012.

Chapter 10
Privacy Enhancing Techniques for the Protection of Mobility Patterns in LBS: Research Issues and Trends

Maria Luisa Damiani

10.1 Introduction

Computing and online services are increasingly being consumed through mobile devices, including smart-phones and tablets. Indeed, more than half of the world population now owns mobile phones, which are capable of running applications in ways that involve the collection, use and sharing of location data.[1] Location-based services (LBS) have become an integral part of users' experiences and an increasingly important market. They deliver to users targeted, relevant and highly convenient information, such as up-to-the-minute traffic reports; the location of the nearest petrol stations, hospitals, or banks; as well as targeted advertisements and coupons for services located in a consumer's immediate range. However, the significant advantages associated with LBS come at a price to users' privacy. While sporadic positions of a mobile device may not be particularly sensitive, the historical trail of past locations, i.e. the user's *trajectory*, can reveal much about a user's behavior. In fact, positioning systems allow constant monitoring of the users' position, both indoors and outdoors; moreover techniques for mobility patterns discovery are increasingly deployed in real applications to summarize users' movement and extract behavioral information, e.g. users' activities, from trajectory data.

Location PETs are privacy enhancing techniques conceived to protect position information from privacy violations in on-line applications. Related literature is rich in location PETs offering solutions to diverse privacy requirements for different typologies of on-line services,[2] such as policy-based location PETs and techniques

[1] Ericsson. Traffic market and data report. Nov. 2011.

[2] John Krumm. "A Survey of Computational Location Privacy" 2009.

M.L. Damiani (✉)
Department of Computer Science, University of Milan,
39, Via Comelico, Milan 20135, Italy
e-mail: damiani@di.unimi.it

S. Gutwirth et al. (eds.), *European Data Protection: Coming of Age*,
DOI 10.1007/978-94-007-5170-5_10, © Springer Science+Business Media Dordrecht 2013

for the protection of *identity privacy* and *location privacy.*[3] In this paper we argue that conventional location PETs do not have the ability to prevent the extraction of behavioral information from trajectory data collected through LBS, mostly because these techniques ignore the context in which users are located. *Position context* plays a fundamental role in the understanding of the users' behavior in pervasive settings.[4] In particular it can reveal what the person is doing, e.g. a person staying in a clinic for a few days is very likely a person who has been hospitalized, while two persons frequenting the same fitness club in the same period, very likely know each other. Preventing the extraction of behavioral information calls for techniques capable of recognizing mobility patterns based on the geographical, temporal and social context.

To support this argument, in what follows we bring examples of behavioral information which can be extracted from trajectory data. Next we discuss the limitations of conventional classes of location PETs. We also consider the aspect of privacy usability,[5] because this is a major requirement for the effective deployment of location PETs, where "usability relates not only to understanding what taking a particular action means in the context of a particular interaction, but also to whether the user understands the implications of his or her choices in a broader context".[6] Finally we introduce recent research on *semantic location privacy* which aims at protecting the *places* (or semantic location) in which users stay, e.g. hospital. These techniques are a first step in the direction of more effective protection of user's behavior.

The rest of the paper is organized in three sections: Sect. 10.2 introduces the application context and privacy requirements; Sect. 10.3 overviews the features of four classes of location PETs, including the aforementioned "conventional" techniques and semantic location privacy techniques; the conclusive Sect. 10.4 covers additional privacy requirements originating from the recent diffusion of positioning services offered by third party providers and reports some final considerations.

10.2 Technological and Application Context

Figure 10.1 illustrates the two main components of a conventional LBS application: (a) a set of location-aware mobile devices, acting as *clients*, i.e. requesters of the information service, which acquire their (accurate) position through a GPS receiver or some other trustworthy location source; (b) The LBS *provider* which acts as *server*, i.e. it responds to the requests of service by providing geo-referenced information tailored to the client's position. The requester of the service specifies its

[3] Christian Jensen et al. "Location Privacy Techniques in Client-Server Architectures". 2009.

[4] Pankaj Mehra. "Context-Aware Computing: Beyond Search and Location-Based Services". 2012.

[5] Giovanni Iachello et al. "End-User Privacy in Human-Computer Interaction". 2007.

[6] Security Steering Committee on the Usability and Privacy of Computer Systems; National Research Council. "Overview of Security, Privacy, and Usability". 2010.

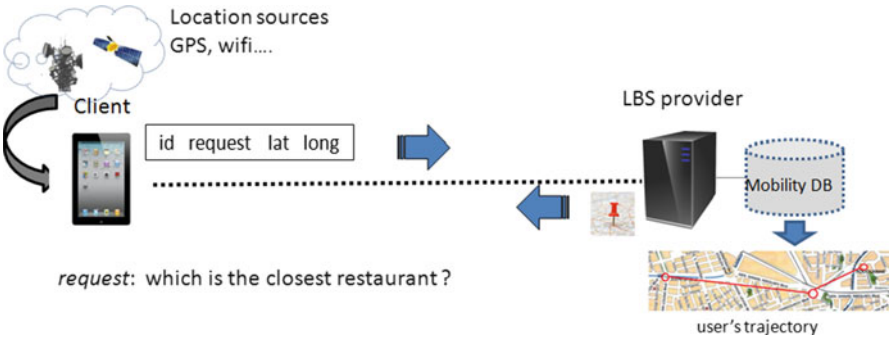


Fig. 10.1 The conventional architecture of a LBS application

identifier, e.g. IP address, the service, e.g. a query, and the position coordinates, e.g. latitude and longitude. The LBS provider stores the position information along with supplementary information in a *mobility database*. A sequence of time-stamped positions forms a user's trajectory.

10.2.1 Extracting Behavioral Information from Trajectory Data in LBS: An Example

In certain applications users are allowed to inspect the content of the mobility database. For example, the users of the location sharing service Google Latitude[7] can use the *Location History* functionality to store, view, and manage their past Latitude locations. Figure 10.2b illustrates the trajectory of a volunteer user running the Latitude application on a smartphone. Following common usage, the device is permanently connected to Internet, while the user's position is constantly monitored by the application running in background. The trajectory, reporting the movement during 1 week in Milan, is displayed as sequence of segments, each connecting two consecutive positions. A dashboard allows inspection of the content, for example, by regulating the time-bar (at the bottom of the picture) one can find where the person was located at a precise instant and how long the person stayed in that position. Moreover, as the trajectory is drawn onto a detailed map, the places that the user visits can be easily identified.

More interesting is Fig. 10.2a which illustrates the statistics that the system provides on the user's activities, in particular the time spent at home, at work and outside. Note that the patterns "home", "work" are inferred from the system based on the movement information. For example, the inactivity periods during night hours can reveal where the user lives, while frequent movements from home to some other place at certain hours can disclose where the user works.

[7] http://www.google.com/latitude.

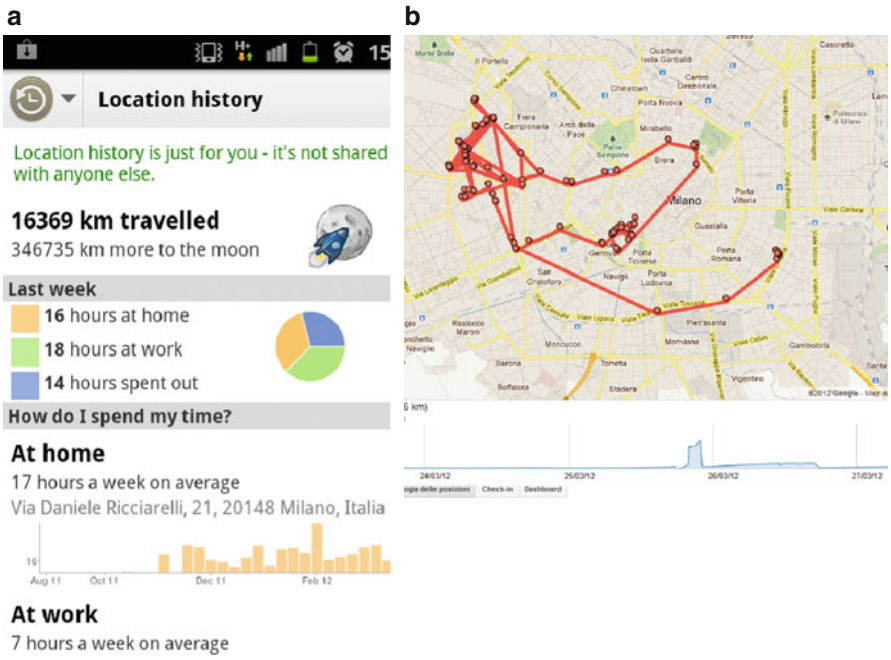


Fig. 10.2 Google location history: movement statistics (**a**) and the trace of an individual (**b**)

While it can be seen that the accuracy of the extracted information is low (e.g. the time spent at home is unrealistic) this example clearly shows the potential of the techniques for mobility patterns discovery. It is also foreseeable that information accuracy will rapidly increase in the near future under the push of on-going research on mobility pattern discovery and representation. On-going research includes, for example, *trajectory pattern mining*[8] which aims at identifying the regions that people usually frequent, how much time is spent in each of those regions and the preferred order in which those regions are visited; *mining of points of interest*[9] i.e. extraction of places that are significantly frequented; *semantic trajectories*[10] which allow the representation of behavioral information in a machine-readable form.

10.2.2 Mobility Patterns

Mobility patterns reveal what people do, i.e. behavioral information. For example, people spend different amount of time in a location depending on what they do there, e.g. a

[8] Fosca Giannotti et al. "Trajectory Pattern Mining". 2007.

[9] Xin Cao et al. "Mining Significant Semantic Locations from GPS Data". 2010.

[10] Stefano Spaccapietra et al. "A Conceptual View on Trajectories". 2008.

user staying in a night-club at nightly hours is likely a customer of the nightspot. This pattern is called *staying duration* in Lee et al.[11] Other interesting examples of patterns, besides the home-work pattern seen in the previous example, are reported in Opinion 13/20111 by the Article 29 Working Party.[12] In particular, patterns may include data derived from the movement patterns of friends as well as "special categories of data", such as visits to hospitals and religious places, presence at political demonstrations or presence at other specific locations revealing data about, for example, sex life. In all these examples, the extraction of behavioral information is leveraged by the intertwining of trajectory data with contextual information such as geographical places, time, frequency, duration of staying, and the social context.

10.3 Privacy Enhancing Techniques for the Protection of Position in LBS

The bulk of research on privacy of position data took off with the emergence of mobile applications based on stored people's tracks,[13, 14] early past decade. Current location PETs can be grouped in two broad classes of solutions. The first class of techniques are commonly referred to as *policy-based*. A *policy* consists of a set of user-defined privacy preferences or *rules* typically enforced by the trustworthy LBS provider upon the request of service. We refer to the second class of solutions as *inference-prevention* techniques. These techniques basically aim at preventing the LBS provider from drawing sensitive information from exact positional data. Note that in this case the LBS provider is considered not fully trustworthy, e.g. cooperative and curious. Taking inspiration from the classification proposed by Jensen et al.,[15] we further categorize inference-prevention techniques in the following classes:

- *Identity privacy* techniques attempt to forestall the re-identification of users (deprived of their real identity) in LBSs providing anonymous services
- *Location privacy* techniques apply to forestall the transmission of *exact* users' positions to the LBS provider. Knowing precisely the positions in which individuals are located (or not located) jeopardizes their privacy and physical safety.
- *Semantic location* privacy techniques aim at preventing the disclosure of the places in which users stay because those locations can reveal sensitive data and behavioral information.

[11] Byoungyoung Lee et al. "Protecting Location Privacy Using Location Semantics". 2011.

[12] Article29 Data Protection Working Party. Opinion 13/2011. 2011.

[13] Mark Gruteser et al. "Anonymous Usage of Location-Based Services Through Spatial and Temporal Cloaking". 2003.

[14] Alastair Beresford et al. "Location Privacy in Pervasive Computing". 2003.

[15] Christian Jensen et al. "Location Privacy Techniques in Client-Server Architectures". 2009.

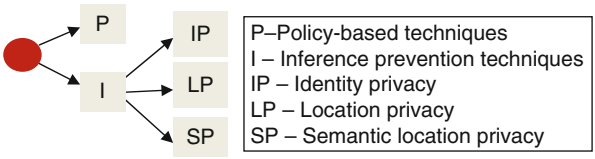


Fig. 10.3 A taxonomy of location PETs

The whole taxonomy is shown in Fig. 10.3. In the next, we examine these four classes of techniques, i.e. policy-based techniques and the three inference prevention techniques. In order to keep the paper focused, we choose not to use any formal privacy and utility metric,[16] while this analysis is postponed for future work.

10.3.1 Policy-Based Techniques

Policy-based techniques are probably the most popular solutions for privacy in LBS, conceptually simple, in line with common practices in law, and endorsed by standardization bodies such as IETF Geopriv.[17] These techniques allow users to specify which location is to be disclosed to whom and when, through a set of machine-readable and enforceable privacy rules. *Machine-readable* means that rules are encoded using a computer language (i.e. a *policy-specification language*) instead of being expressed in natural language; *enforceable* means that those rules can be checked by an automated system, on behalf of the user. These techniques have their roots in security, in particular in access control policies, and in the bulk of work developed at the end of 1990s for privacy protection in e-commerce applications, i.e. P3P.[18]

As an example, consider the case in which the user John wants to share his location with acquaintances through a location sharing service constantly monitoring the user's position. Because acquaintances include colleagues, relatives, and friends, John chooses to specify different rules, one for each category. A rule can state for example that John's position can be revealed to colleagues Bob and Mary exclusively when John is at work and during working-time. The set of rules forms the John's privacy policy. For example, this technique is used in the Locaccino location sharing service.[19] In particular, the subscribers of this service can specify privacy rules encompassing both temporal conditions and spatial conditions, i.e. the periods and the regions within which the position can be disclosed or hidden to acquaintances. These rules are enforced by the Locaccino server.

[16] Reza Shokri et al. "Quantifying Location Privacy". 2011.

[17] IETF. "An Architecture for Location and Location Privacy in Internet Application". 2011.

[18] Lorrie Cranor. "*P3P*: Making Privacy Policies More Useful". 2003.

[19] Eran Toch et al. "Locaccino: A Privacy Centric Location Sharing Appplication". 2010.

Discussion

Policy-based techniques do not prevent the extraction of mobility patterns because the LBS provider is generally aware of the positions of all clients and thus can record users' trajectories at the finer level of detail. Therefore, if the LBS provider is untrustworthy, the user's privacy is at stake. However policy specification languages have a peculiar feature, i.e. the capability of expressing conditions on contextual variables. The degree of usability of these languages is generally assessed by involving users in the experimentation. For example, Tsai et al. report the positive feedback of a group of selected users requested to use solely time-based privacy rules such as: "Show my location between 9 am and 6 pm on Mondays and Wednesdays".[20]

10.3.2 Identity Privacy Techniques

Identity privacy techniques are conceived to forestall the re-identification of seemingly anonymous users, based on position information. For example, consider the case in which an LBS is offered to the members of a community potentially subject to discrimination, e.g. the gay community, and assume users to interact with the system through pseudo-identifiers. Unfortunately simply stripping off users' identifiers is not sufficient to ensure anonymity, because the LBS provider can draw users' identities from trajectory information, e.g. if a user requests the service from a certain place early in the morning, it is likely that such a place is his or her home and thus the user can be easily re-identified using a white pages service.[21] While we refer the reader to Chow et al. for a recent survey on trajectory privacy,[22] we limit ourselves to consider an exemplifying paradigm, i.e. *location k-anonymity*.

Given a population of users, location k-anonymity postulates the following requirement, that the user's location disclosed to the LBS provider must be indistinguishable from the location of at least k-1 other users. In practice, the exact user's location must be replaced by a coarser position, i.e. a *cloaked* region, large enough to contain the position of *k-1* other users located nearby at the time the on-line service is requested. Accordingly, the LBS provider cannot identify the requester of the service based exclusively on the position information. This situation is exemplified in Fig. 10.4. For k = 10, the position of the single individual is replaced by a larger region (i.e. a cloaked region) containing 10 persons. If the on-line service is requested from this region, the maximum probability of identifying the requester is 1/10. Another prominent feature of this privacy mechanism is that it typically requires a dedicated trusted middleware, the *location anonymizer*, in between the clients and

[20] Tsai, Janice et al. "Who's Viewed You?: The Impact of Feedback in a Mobile Location-Sharing Application". 2009.

[21] Mark Gruteser et al. "Anonymous Usage of Location-Based Services Through Spatial and Temporal Cloaking". 2003.

[22] Chi-Yin. Chow et al. "Trajectory Privacy in Location-Based Services and Data Publication". 2011.

Fig. 10.4 A cloaked region for K = 10

Fig. 10.5 The Casper system

the LBS provider. The location anonymizer is aware of the position of all the clients, intercepts the individual's requests, replaces the user's identifier with a pseudo-identifier and finally replaces the true position with the dynamically generated cloaked region. One representative solution of this class is the Casper system[23] (Fig. 10.5). Casper consists of the location anonymizer and the *privacy-aware query processor*, a software component which runs on the server (i.e. the LBS provider), and which resolves user's requests with respect to a position which is not a point as usual, but a region and which returns a set of candidate answers. Although alternative architectures have been proposed,[24] the practical deployment of location k-anonymity in real applications looks complex and costly.

Discussion

Location k-anonymity techniques do not forestall the extraction of mobility patterns from trajectory data (even though trajectories have a coarse granularity), because the position context is ignored. For example, cloaked regions are generated independently from the geographical setting. Consequently, if a cloaked region falls

[23] Mohamed Mokbel et al. "The New Casper: Query Processing for Location Services Without Compromising Privacy". 2006.

[24] Gabriel Ghinita et al. "MobiHide: A Mobile Peer-to-Peer System for Anonymous Location-Based Queries". 2007.

inside the area covered by a hospital, one can infer that the k users grouped in the region suffer from health concerns. Hence, if users are re-identified, there is a privacy leak. In essence, location k-anonymity only serves to protect the association between users and service requests. Another consideration regards usability. It is difficult to gauge which size of k is minimally necessary or sufficient.[25] The higher the value of k, the higher the level of protection but also the loss of position accuracy (and thus of quality of service, *QoS*), where the position accuracy varies in time and space based on the distribution of people.

10.3.3 Location Privacy Techniques

Location privacy techniques aim at preventing the disclosure of exact users' location in the context of LBSs possibly providing non-anonymous services, for example geo-social networks.[26] These techniques communicate to the LBS provider a location other than the exact position. In particular, the disclosed position can be fake, cloaked or can be transmitted using some cryptographic protocol.

- A *fake position* is a position deliberately represented with a wrong value. Privacy is achieved from the fact that the reported position is false. The accuracy and the amount of privacy mainly depend on how far the reported location is from the exact location. For example, the client requesting a service, e.g. "where is the closest restaurant" can transmit to the LBS provider a fake position and then properly filter out candidate answers.[27]
- A*n obfuscated position* is another term for cloaked region. Therefore the LBS provider does know that the user is located in the cloaked region, but has no clue where exactly the user is located. A popular obfuscation method,[28] also used in commercial platforms,[29] replaces the actual position with a predefined region chosen in a taxonomy of locations at different granularities e.g. street, zip code area, city. Unfortunately predefined locations can be too broad to ensure an appropriate QoS, say a zip code region covering an area of few squared kilometers, or conversely too small to provide privacy guarantees, say a short street. Another simple method obfuscates the position with a circle of user-defined radius and random center containing the actual position.[30] In more complex

[25] Mark Gruteser et al., 2003, see note 19.

[26] Carmen Ruiz Vicente et al. "Location-Related Privacy in Geo-Social Networks". 2011.

[27] Man Lung Yiu et al. "SpaceTwist: Managing the Trade-Offs Among Location Privacy, Query Performance, and Query Accuracy in Mobile Services". 2008.

[28] IETF, 2011, see note 16.

[29] http://fireeagle.yahoo.net/.

[30] Claudio Ardagna et al. "Location Privacy Protection Through Obfuscation-Based Techniques". 2006.

solutions, the size of the cloaked region is the result of the trade-off between privacy and QoS[31] while the transmission of the location can be also delayed a while to cloak the temporal dimension.[32]

– Cryptographic protocols define techniques for the secure collaboration of different parties. An example of *cryptographic protocol* used in LBS is PIR (Private Information Retrieval). This technique allows users to issue a query without disclosing to the LBS provider the information which is requested as well as the information being returned.[33] In this sense this technique protects both the identity and the location. The method ensures the maximum privacy. However it incurs high computational costs and can be only applied to certain categories of queries, e.g. the retrieval of stationary objects (i.e. non-mobile objects).

One specific problem that may rise when the position is obfuscated by a coarse region is that consecutive positions in the user's trajectory are correlated, i.e. the presence in one region constrains the position in the subsequent regions. This information can be exploited to prune the cloaked regions and more precisely delimitate the user's position. To prevent this inference when the maximum speed of the user is known (e.g., the user can be a pedestrian, a car driver, a cyclist and so on) and the movement is frequently sampled, an approach is to modify the position in space and time before it is released.[34]

Discussion

In general, location privacy techniques are not able to prevent the extraction of mobility patterns. The solutions based on obfuscation and fake positions have the same limitations discussed in the previous section, i.e. lack of context awareness, while the deployment of cryptographic protocols in LBS is somewhat limited to specific situations or applications. As concerns the aspect of usability, obfuscation techniques are the simplest but not necessarily usable solutions. For example, what is the loss of QoS if the position is disclosed at the level of zip code area, instead of street? The lack of suitable metrics makes it difficult understanding the implications of certain choices.

[31] Marc Duckham et al. "A Formal Model of Obfuscation and Negotiation for Location Privacy". 2005.

[32] Reynold Cheng et al. "Preserving User Location Privacy in Mobile Data Management Infrastructures". 2006.

[33] Gabriel Ghinita et al. "Private Queries in Location Based Services: Anonymizers Are Not Necessary". 2008.

[34] Gabriel Ghinita et al. "Preventing Velocity-Based Linkage Attacks in Location-Aware Applications". 2009.

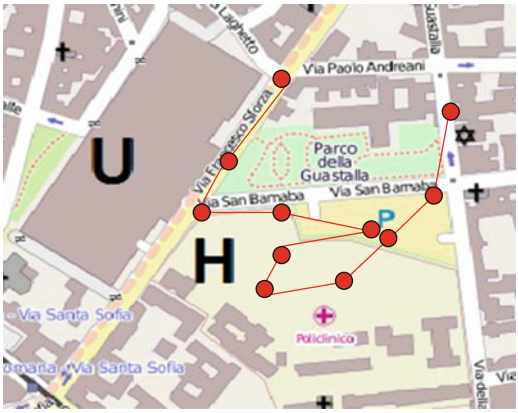


Fig. 10.6 Urban setting and Bob's route (The map is drawn from http://www.openstreetmap.org)

10.3.4 Semantic Location Privacy Techniques: A First Step Towards the Protection of Behavioral Information

Semantic location privacy techniques attempt to prevent LBS providers from identifying the semantic locations in which users stay.[35, 36] For example, one of the motivating observations is that the sensitivity of positions may vary depending on the nature of places, e.g. the position of a user staying in an oncological clinic is likely "more sensitive" than the position of an user walking along a street. Indiscriminately treating every position by imposing the maximum level of privacy for each position would compromises QoS. A more flexible solution is to protect only those positions which are perceived as sensitive, while the others that are not sensitive are disclosed with no change. In this way the loss of QoS can be limited. This form of obfuscation is called *semantic location cloaking*.

As an example, consider the urban setting in Fig. 10.6. The map shows a number of places in Milan: the premises of the Policlinico hospital, the University of Milan, a few religious buildings, various private buildings, and the road network. Assume that the user Bob connects to a location sharing service through a smartphone. Bob is driving his car when in the proximity of the Policlinico hospital, Bob stops in a parking area and steps onto the hospital premises where he remains for a few hours for a medical visit, before again taking the car to reach his friends in a pub in downtown. During this time, Bob's position is continuously reported to the LBS provider

[35] Byoungyoung Lee et al. "Protecting Location Privacy Using Location Semantics". 2011.

[36] Maria Luisa Damiani et al. "Fine-Grained Cloaking of Sensitive Positions in Location Sharing Applications". 2011.

as well as his friends, therefore the places in which Bob stops are known, including those that Bob consider sensitive, e.g. the hospital. Simply disconnecting from the service would prevent Bob from being in touch with his friends, unless suspending and then resuming the service which would create considerable burden to Bob. The issue is how not to reveal to the LBS provider that the user certainly stays in a certain place, without giving up the service.

To illustrate the technical issue posed by this problem, consider first a naive solution. Assume a user in position p. Upon a request of service, the main steps of the privacy enforcement process are:

1. The client checks whether p is within one of the places considered sensitive (assume there is a precompiled list of sensitive places, e.g. hospitals, religious buildings and a map on the client)
2. If this is the case, generate a cloaked region containing the actual position
3. Otherwise, if the user is not in a sensitive place, release the actual position

It is easy to see that, if the LBS provider is aware of the protection strategy, it can promptly infer from the fact that Alice is in a cloaked region that she is certainly inside a sensitive location. Moreover, if the party has clues about the sensitive locations, she can more precisely localize Alice inside the cloaked region. As a result the protection mechanism fails. In previous work[37] we argued that a sound cloaking strategy should guarantee:

- **Semantic diversity**. The user's position cannot be blurred exclusively when the user is inside a sensitive place, but also when he or she is outside. That way, the place in which the user is located remains uncertain. A cloaked region thus must include places of diverse types.
- **Independence** of the position cloaking method from the user's position. This condition prevents the discovery of the correlation between the cloaked region and the true position, which could be exploited to infer where the user is located.

These guidelines have been embodied in the privacy-preserving framework called Probe (Privacy-aware Obfuscation Environment).[38] Figure 10.7a illustrates the workflow of the privacy enforcement process. Users first specify in a privacy profile which categories of points of interest are sensitive (selecting for example from a pre-defined list, e.g. hospitals, religious buildings and so on) along with the degree of privacy desired for each of those categories. For example a privacy degree of 0.1 assigned to hospitals means that the (posterior) probability of locating the user inside a hospital must be less than 0.1. Next, coarse regions are generated satisfying the privacy preferences, independently from the user's position, in order to prevent possible inferences on their reciprocal positions. A sample set of cloaked regions is shown in Fig. 10.7b. Finally, at runtime if the user's position falls inside

[37] See note 36.

[38] Maria Luisa Damiani et al. "The PROBE Frame Work for the Protection of Sensitive Positions". 2010.

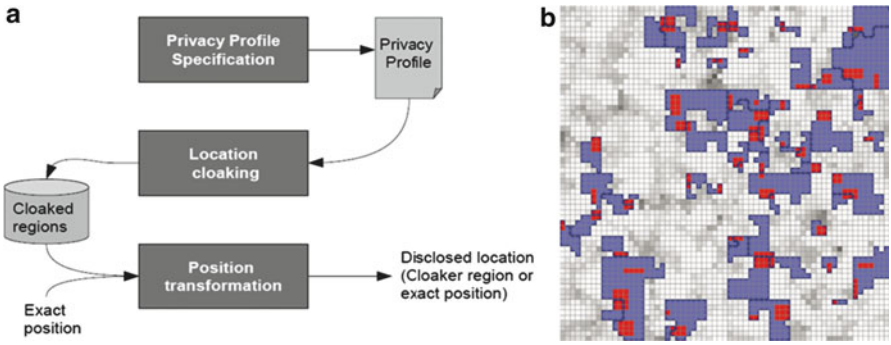


Fig. 10.7 Probe system: (**a**) the workflow; (**b**) obfuscated map: the *blue polygons* represent cloaked regions, the *red rectangles* sensitive places, the *grey background* the distribution of population in space

one of the coarse regions, that region is delivered instead of the exact position. Recent results extend these techniques to the case in which users' movement is confined to road network.[39] In this case the cloaked region takes the form of a subgraph of a semantically annotated graph representing the urban setting.

Discussion

The concern for semantic location privacy is recent and thus many research issues are still open. For example, an issue is how to intertwine the geographical context with the temporal and social dimension; another problem regards the protection of interrelated places, e.g. the home-work pattern. As concerns usability, no study has been carried out on this aspect. However, in the specific case of the PROBE system, users can specify their privacy preferences in a privacy profile using an intuitive and conceptually founded privacy metric. Moreover an additional metric is defined, the utility metric, providing a measure of the spatial accuracy of the cloaked regions. Unlike more traditional obfuscation techniques, the utility measure can be computed prior to any service request. In this way users can tune and balance the amount of privacy with QoS.

10.4 Open Issues and Conclusions

10.4.1 Towards a More Complex LBS Model

All the location PETs that we have considered so far, including the most recent techniques, rely on the assumption that the location information is obtained from some trusted source, such as GPS. Indeed, LBSs are rapidly evolving towards novel

[39] Emre Yigitoglu et al. "Privacy-Preserving Sharing of Sensitive Semantic Locations Under Road Constraints". 2012.

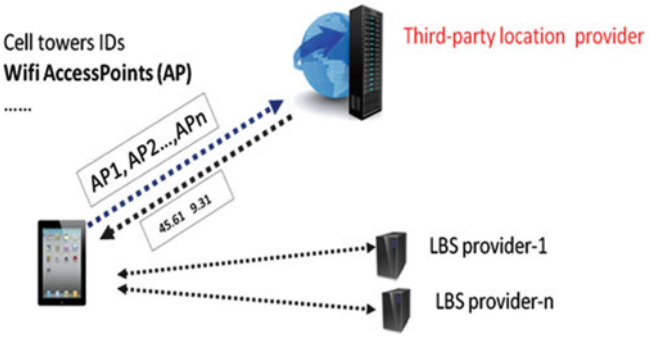


Fig. 10.8 LBS model extended with the third party location provider

architectures in which the position information can be pervasively offered by third-party location providers (LP). The location service is offered on a free basis provided that users reveal contextual information, e.g. Wi-Fi networks nearby. Currently, LPs include all major IT players, such as Google and Apple. We postulate that, in the same way of LBS providers, LPs are not necessarily trustworthy.

10.4.1.1 Architecture and Problem Formulation

Figure 10.8 depicts the extended LBS model comprehensive of the third party location provider. A usage scenario is as follows. Assume that a user, equipped with a Wi-Fi enabled device and located in a metropolitan area (with high density of Wi-Fi networks), requests a LBS. The application running on the client handles this request as follows:

- It first determines the position of the device. Since the user is inside a building and thus the GPS signal is not available (or the GPS receiver is not installed), the position is requested from the LP. To obtain the position, the client transmits to the LP the set of Wi-Fi access points (APs) and/or the cell towers in proximity of the device. In a metropolitan area, the position can be computed with an accuracy of a few tens of meters.
- Once the coordinates are obtained, the application conveys the position along with the requested service to the LBS provider which returns the requested information as usual.

In this scenario, it is obvious that the LP is necessarily aware of the user's location. Moreover, if the client interacts with a unique LP, such LP is aware of any position flowing to the LBS providers. Now consider the case in which the LP is untrustworthy. It should be clear that existing location PET cannot protect the position from the LP which computes it. Therefore the problem is to what extent privacy can be protected without giving up the LBS and compromising the business model (entailing free access to the LP).

10.4.1.2 Problem Analysis

If the client could determine by itself the position with sufficient accuracy both indoors and outdoors, there would not be privacy concerns. Unfortunately providing clients with pervasive geo-location capabilities is costly. We argue that a different approach is to minimize the interaction with the LP. The motivating observation is that the amount of information that the user transmits to the location provider exceeds what is really necessary to determine the users' position. For example every time a service is requested from a place, e.g. home, the client transmits the same or similar contextual information, e.g. Wi-Fi networks in proximity, even though the position has been already obtained the first time a request has been made from that place. Based on this observation, we envision a solution in which enhanced clients can acquire the capability of recognizing places that have been already visited. This way the position is only requested to the LP when it is strictly necessary. We qualify this geo-location service as *privacy-aware*.

To implement this strategy a possible approach is to confine the protection to a subset of positions, in particular those which can be associated with *private places.*[40] Private place is an abstraction which conceptualizes the intuition that there are some regions of space that belong to the personal sphere, e.g. home. Whenever the user is in a private space, the position is not disclosed to the LP.

Note, however, that this solution does not forestall the disclosure of the position to the LBS provider. Therefore for a comprehensive approach, privacy-aware geo-location and (context-aware) location PETs should be integrated.

10.4.2 Concluding Remarks

We conclude with two summarizing considerations:

1. We have seen that location PETs include a variety of techniques conceived to satisfy different privacy requirements. In general, conventional techniques are not able to prevent the extraction of mobility patterns from trajectory data. We have also outlined the features of a recent stream of research for the protection of presence in places, which attempts to introduce the contextual dimension in privacy. This experience can be extended along several directions, for example to account for the temporal and social dimension of privacy. Another interesting research direction regards the combined use of policy specification languages and inference prevention techniques.
2. The architecture and inner workings of current LBS ecosystem remain opaque and largely unknown to users. For example, users often do not know that while they interact with and authorize a specific online or mobile application (Apps) to determine their location, such an App refers to a LP to obtain the localization

[40] Maria Luisa Damiani. "Third Party Geo-Location Services: Privacy Requirements and Research Issues". 2011.

service. Like many other privacy and data protection problems, transfers of data to LPs need to be addressed through a combination of legal and technological mechanisms. Technological solutions can provide users even more robust privacy protections than legal rules. However, protecting mobility patterns from location providers and LBS providers especially if both parties are untrustworthy, is a challenge.

References

Ardagna, Claudio, Marco Cremonini, Ernesto Damiani, Sabrina De Capitani di Vimercati, and Pierangela Samarati. 2007. Location privacy protection through obfuscation-based techniques. In *Proceedings of the 21st annual IFIP WG 11.3 working conference on data and applications security*, Redondo Beach, July 2007.

ARTICLE 29 Data Protection Working Party. 2011. Opinion 13/2011 on Geolocation services on smart mobile devices. http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp185_en.pdf. Last visit: July 2012.

Beresford, Alastair, and Frank Stajano. 2003. Location privacy in pervasive computing. *IEEE Pervasive Computing* 2: 46–55.

Cao, Xin, Gao Cong, and Christian S. Jensen. 2010. Mining significant semantic locations from GPS data. *Proceedings of VLDB Endow* 3(1–2): 1009–1020.

Chow, Chi-Yin, and Mohamed Mokbel. 2011. Trajectory privacy in location-based services and data publication. *SIGKDD Explorations* 13(1): 19–29.

Cranor, Lorrie. 2003. P3P: Making privacy policies more useful. *IEEE Security and Privacy* 1(6): 50–55.

Damiani, Maria Luisa. 2011. Third party geo-location services: Privacy requirements and research issues. *Transaction on Data Privacy* 4(2): 55–72.

Damiani, Maria Luisa, Elisa Bertino, and Claudio Silvestri. 2010. The PROBE framework for the personalized cloaking of private locations. *Transactions on Data Privacy* 3(2): 123–148.

Damiani, Maria Luisa, Claudio Silvestri, and Elisa Bertino. 2011. Fine-grained cloaking of sensitive positions in location sharing applications. *IEEE Pervasive Computing* 10(4): 64–72.

Doty, Nick, Deirdre Mulligan, and Erik Wilde. 2010. Privacy issues of the W3C Geolocation API. Technical report, UC Berkeley, School of Information, Berkeley.

Duckham, Matt, and Lars Kulik. 2005. A formal model of obfuscation and negotiation for location privacy. In *Pervasive computing.* Berlin/Heidelberg: Springer, 152–170.

Ericsson, Traffic market and data report. Nov. 2011. http://www.ericsson.com/res/docs/2012/tmd_report_feb_web.pdf. Last visit: July 2012.

Ghinita, Gabriel, Panos Kalnis, and Spiros Skiadopoulos. 2007. MobiHide: A mobile peer-to-peer system for anonymous location-based queries. In SSTD, 221–238, Boston.

Ghinita, Gabriel, Panos Kalnis, Ali Khoshgozaran, Cyrus Shahabi, and Kian-Lee Tan. 2008. Private queries in location based services: Anonymizers are not necessary. In *Proceedings of the ACM SIGMOD international conference on management of data.* Vancouver, Canada.

Ghinita, Gabriel, Maria Luisa Damiani, Claudio Silvestri, and Elisa Bertino. 2009. Preventing velocity-based linkage attacks in location-aware applications. In *Proceedings of the ACM international conference on advances in geographic information systems*. New York: ACM.

Giannotti, Fosca, Mirco Nanni, Fabio Pinelli, and Dino Pedreschi. 2007. Trajectory pattern mining. In *ACM SIGKDD international conference on knowledge discovery and data mining,* New York: ACM.

Gruteser, Mark, and Dirk Grunwald. 2003. Anonymous usage of location-based services through spatial and temporal cloaking. In *Proceedings of the 1st international conference on mobile systems, application and services,* San Francisco.

Iachello, Giovanni, and Jason Hong. 2007. End-user privacy in human-computer interaction. *Foundations and Trends in Human-Computer Interaction* 1(1): 1–137.

IETF, Request for Comments 6280. 2011. An architecture for location and location privacy in internet application. http://tools.ietf.org/html/rfc6280. Last visit: July 2012.

Jensen, Christian S., Hua Lu, and Man Lung Yiu. 2009. Location privacy techniques in client-server architectures. In *Privacy in location-based applications*, Bettini, Claudio, Sushil Jajodia, Pierangela Samarati, and X. Sean Wang, ed. Lecture Notes in Computer Science, vol. 5599, 31–58. Berlin/Heidelberg: Springer.

Krumm, John. 2009. A survey of computational location privacy. *Personal and Ubiquitous Computing* 13(6): 391–399.

Mehra, Pankaj. 2012. Context-aware computing: Beyond search and location-based services. *IEEE Internet Computing* 16(2): 12–16. March–April, 2012.

Mokbel, Mohamed, Chin-Yin Chow, and Walid Aref. 2006. The new Casper: Query processing for location services without compromising privacy. In *Proceedings of very large database conference*. Seoul, Korea.

Security Steering Committee on the Usability and Privacy of Computer Systems, National Research Council. 2010. Overview of security, privacy, and usability. In *Toward better usability, security, and privacy of information technology: Report of a workshop*. Washington, D.C.: The National Academies Press.

Shokri, Reza, George Theodorakopoulos, Jean-Yves Le Boudec, and Jean-Pierre Hubaux. 2011. Quantifying location privacy. In *IEEE symposium on security and privacy*, 247–262. Oakland, CA, USA.

Toch, Eran, Justin Cranshaw, Paul Hankes-Drielsma, Jay Springfield, Patrick Gage Kelley, Lorrie Cranor, Jason Hong, and Norman Sadeh. 2010. Locaccino: A privacy-centric location sharing application. In *Proceedings of the 12th ACM international conference on Ubiquitous computing*. Copenhagen, Denmark.

Tsaj, Janice, et al. 2009. Who's viewed you?: The impact of feedback in a mobile location-sharing application. In *Proceedings of the 27th international conference on human factors in computing systems (CHI '09)*. Boston, USA.

Vicente, Carmen Ruiz, Dario Freni, Claudio Bettini, and Christian Jensen. 2011. Location-related privacy in geo-social networks. *IEEE Internet Computing* 15(3): 20–27.

Ygitoglu, Emre, Maria Luisa Damiani, Osman Abul, and Claudio Silvestri. 2012. Privacy-preserving sharing of sensitive semantic locations under road constraints. In *IEEE international conference on mobile data management*, July 2012. Bengalore, India.

Yiu, Man Lung, Christian S. Jensen, Xuegang Huang, and Hua Lu. 2008. SpaceTwist: Managing the trade-offs among location privacy, query performance, and query accuracy in mobile services. In *Proceedings of the IEEE 24th international conference on data engineering (ICDE '08)*. Cancun, Mexico.

Chapter 11
Privacy by Design Through a Social Requirements Analysis of Social Network Sites form a User Perspective

Ralf De Wolf, Rob Heyman, and Jo Pierson

11.1 Introduction

When looking at contemporary digital society we see that personal communication and mass communication are converging.[1] Through this process, new kinds of platforms for social interaction are created, such as Social Network Sites (SNS), e.g. Facebook, Twitter, MySpace. Especially adolescents seem to be drawn to these sites. Most of the American adolescents are online and 80% are active on SNS,

SPION (Security and Privacy for Online Social Networks) (www.cosic.esat.kuleuven.be/spion) is a 4-year project (1/1/2011–31/12/2014) in the SBO programme for strategic basic research with societal goal, funded by IWT (government agency for Innovation by Science and Technology) in Flanders (Belgium). The research project is a cooperation between COSIC/ESAT/Department of Electrical Engineering (K.U.Leuven), DISTRINET/Department of Computer Science (K.U.Leuven), DTAI/Department of Computer Science (K.U.Leuven), ICRI/Faculty of Law (K.U.Leuven), IBBT-SMIT/Department of Communication Studies (Vrije Universiteit Brussel), OWK/Department of Educational Studies (Universiteit Gent) and Heinz College (Carnegie Mellon University), coordinated by KUL-COSIC.

EMSOC (User Empowerment in a Social Media Culture) (www.emsoc.be) is a 4-year project (1/12/2010–30/11/2014) in the SBO programme for strategic basic research with societal goal, funded by IWT (government agency for Innovation by Science and Technology) in Flanders (Belgium). The research project is a cooperation between Vrije Universiteit Brussel (IBBT-SMIT & LSTS), Universiteit Gent (IBBT-MICT & C&E) and Katholieke Universiteit Leuven (ICRI & CUO), coordinated by IBBT-SMIT.

[1] Manuel Castells, *Communication Power*. (Oxford: Oxford University Press, 2009).

R. De Wolf (✉) • R. Heyman • J. Pierson
IBBT-SMIT, VUB, 9, Pleinlaan, 1050 Brussels, Belgium
e-mail: ralf.de.wolf@vub.ac.be; rob.heyman@vub.ac.be; jo.pierson@vub.ac.be

S. Gutwirth et al. (eds.), *European Data Protection: Coming of Age*,
DOI 10.1007/978-94-007-5170-5_11,

according to Pew Research Center.[2] The third wave of the Digimeter[3] states that 58.8% of the online population in Flanders has an account on a SNS. The claim of Deuze[4] that people tend to be living more 'in media' than 'with media' lies closer to the truth than we would think. This transition to mass self-communication brings along not only opportunities, but also risks for the user.

We consider these technologies as empowering for the user, building up an online identity and managing their social network. However, SNS are often contested because of privacy issues. In literature a distinction is made between social privacy and instrumental privacy in SNS. Social privacy is defined as the '*control of information flow about how and when personal information is shared with other people.*'[5] Context collision[6] or context collapse[7] represent such problems from the perspective of social privacy. It refers to the blurring of contexts in an online environment, whereas in an offline environment more or less strict barriers can be distinguished. Instrumental privacy refers to personal data being accessed by governments and corporations, e.g. using data mining and related statistical analysis methods.[8] This distinction makes us aware of the different nature of privacy problems on SNS. A notion that should also be translated in possible solutions. However these privacy definitions are not optimal, because the role of the user in both definitions is left undefined and the interconnection between both concepts is overlooked. The user as social being can therefore act in an instrumental manner as well. Rather, we propose to make a distinction between 'privacy as subject' and 'privacy as object'. In 'privacy as subject' we allocate a more or less active role to the user. We consider the user as an active subject defining who can and cannot see her personal information flow. It is not just about the information flow *an sich*, but also on using this information for creating meaning in a social context. In 'privacy as object' we consider the user as undergoing social reality and state that the information considered here is part of a bigger economic system. The disclosure of information is needed to obtain another result. For example, we need to disclose personal information to an online form in order to purchase something. Throughout this paper 'privacy as subject' and 'privacy as object' will be used.

Taking the two privacy conceptions together we see a common trend where the responsibility is pushed towards the individual user, who often does not – or cannot – question the technology he is using. This phenomenon is indicated as the

[2] Pew Internet & American Life Project, http://pewinternet.org.

[3] Digimeter, http://digimeter.be.

[4] Mark Deuze, "Media life." (*Media, Culture and Society 33*, 2011), 137–148.

[5] Kate Raynes-Goldie, "Aliases, creeping, and wall cleaning: Undertanding privacy in the age of Facebook," *First Monday 15* (2010), accessed November 30, 2011, http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/viewArticle/2775/2432.

[6] Raynes-Goldie, "Aliases creeping."

[7] Danah Boyd, "Taken out of context: American teen sociality in networked publics" (Ph.D. diss., University of California, 2008).

[8] Danah Boyd and Eszter Hargittai, "Facebook privacy settings: who cares?" *First Monday 15* (2010), accessed November 30; 2011, http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/viewArticle/3086/2589.

responsibilization of individuals. In this paper we focus on reversing the process of responsibilization. Three different strategies can be used to accomplish this. We could focus on filling the gaps and shortcomings of the existing legal framework of SNS or making the user aware of the privacy problems. But the strategy that is applied in this paper is one of embedding privacy, both where the user is subject and object, into the design of technologies that are being developed.

At a theoretical level, we elaborate upon a social constructionist view on technology and introduce the concept of Privacy by Design (PbD). It is our intention to contribute to the process of privacy requirement engineering by capturing the practices and skills of the user, which we define as 'social requirements'. We consider the seven laws of identity proposed by Kim Cameron[9] as a good starting point in capturing and integrating the human user into technology. However, there are also some gaps and shortcomings in these seven laws, that we would like to address. At the empircal level, we combine existing literature together with our own research on social requirements to propose four identity claims, in order to further optimize the laws of identity. With this we are able to propose an integrated approach to PbD and privacy enhancing technologies.

11.2 Social Construction of Technology

11.2.1 Privacy by Design and Social Requirements

'*Privacy by Design refers to the philosophy and approach of embedding privacy into the design specifications of various technologies*', as reported by Cavoukian.[10] Ann Cavoukian, the Information and Privacy Commissioner of Ontario (Canada), is a prominent advocate of this concept. She describes seven principles that should be taken into account in the design process of technologies, whereby privacy can be ensured. We see a clear interconnection between PbD and the notion of Constructive Technology Assessment, as part of the social construction of technology perspective, which will be elaborated upon in Sect. 11.4.3. Technology Assessment (TA) can be regared as '*a scientific, interactive and communicative process which aims to contribute to the formation of public and political opinion on societal aspects of sciences and technology.*'[11] Constructive Technology Assessment (CTA), as a TA subdomain, refers to (advice) on interventions in early stages of technology development based on the assessment of possible problems and risks these technologies could pose for society.[12]

[9] Kim Cameron, "The laws of identity", Kim Cameron's Identity Weblog.

[10] Ann Cavoukian. *Privacy by Design: take the challenge*. Information and Privacy Commissioner of Ontario, Canada, 2009.

[11] European Parliamentarytechnology assessment, http://eptanetwork.org/what.php.

[12] Wim Smit and Ellen van Oost. *De Wederzijds beïnvloeding van technologie en maatschappij – een technology assessment-benadering,* (Bussum: Uitgeverij Coutinho, 1999).

PbD aims to be a holistic and a human-orientated term, but often accused of being an empty concept. '*Despite the comprehensiveness, it is not clear from Cavoukian's document what "privacy by design" actually is and how it should be translated into the engineering practice.*'[13] In this paper we do not want to focus on the PbD concept *as such*, but on how it interconnects with one of its applications areas, namely identity, privacy and technology. In a subsection she describes the seven laws of identity formulated by Kim Cameron, applied to the privacy by design concept. '*The privacy-embedded Laws of identity are intended to inject privacy considerations into discussions involving identity – specifically, into the merging technologies that will define an interoperable identity system.*'[14] What is needed is an identity metasystem, *which* '*could make it easier for users to stay safe and in control when accessing resources on the Internet.*'[15]

When looking at web 2.0 applications we notice that the identity layer seems to have nested itself permanently on the Internet. SNS, especially, make it possible to present the own identity online, taking communication processes to a whole new level. We aim to apply the identity metasystem in designing the architecture of SNS, which should lead to a more privacy safe environment when dealing with mass self-communication.

We operationalize the concept of PbD through the process of requirement engineering. '*Requirement engineering is concerned with the transformation of needs expressed in natural language into language that is precise enough to engineer systems.*'[16] It is beyond the scope of this paper to propose functional or even technical requirements, that are precise enough to transform into usable technologies. Instead we will focus on the social requirements of technologies, using the domestication framework.[17]

A domestication framework looks at the use and integration of technologies in the everyday life of users. Under this approach, technologies are studied in the context in which they are used. A central concept within the domestication framework is consumption. Van Den Broeck[18] states that '… *our domestic lives are more and more defined by our consumption of objects and meanings.*' Technologies are not

[13] Seda Gürses, Carmela Troncoso and Claudia Diaz,"Engineering Privacy by Design", (Paper presented at the annual CPDP conference, Brussels, January 29–30, 2011).

[14] Ann Cavoukian, "Privacy by Design."

[15] Ann Cavoukian, "Privacy by Design."

[16] Seda Gürses et al.,"Engineering Privacy."

[17] Roger Silverstone and Leslie Haddon. "Design and domestication of infomration and communication technologies: technical change and everyday life", in *Communication by design: the politics of information and communication technologies*, ed. Robin Mansell and Roger Silverstone. (Oxford: Oxford University Press, 1996): 44–47. – Thomas Berker, Maren Hartmann, Yves Punic and Katie Ward. *Domestication of media and technology.* (Berkshire, Open University Press, 2005): 255.

[18] Wendy van den Broeck, "From analogue to digital: the silent (r)evolution? A qualitative study on the domestication of interactive digital television in flanders." (Ph.D. dissertation, Free University of Brussels, 2011)

floating around in an empty space but are embedded in the everyday life of users. Not everyone consumes technologies in the same manner. Different meanings are instead attached to technology by the user. In other words, technologies are socially constructed in the practices of the users, in line with the social construction perspective in Science and Technology Studies.[19] By studying how the latter is consumed we get a grip on the social requirements of technology. This can be defined as the '*requirements that are extracted from the social background of everyday life of people, with an emphasis on groups or communities and the social practices within*.'[20] The concept of social requirements can be explained more thoroughly when contrasting them with user requirements, also known as classic human-computer interaction. User requirements focus on the direct needs of the (individual) user in relation to the product itself. Whereas, social requirements focus on the needs of the user of an application in interaction with other users. We prefer the term social requirements because identity is our scope of analysis and identity becomes meaningless if it is reduced to the actions of one person only.

11.2.2 Seven Laws of Identity

The seven laws of identity were developed by Kim Cameron who was at that time Identity and Access Architect for the Microsoft Corporation. His motivation for writing this document went further than the task he was given by Microsoft. Cameron formulates seven laws or requirements that should be present in identity related services in order to succeed as a trusted service. These laws have been adapted in An Cavoukian's PBD book[21] and in Microsoft's identity metasystem.[22] This demonstrates that they are practical enough to be implemented. But are they also good enough to enable privacy control by users involved in mass self-communication?

Although Cameron refers to laws, we can easily interpret these guidelines as requirements because they always refer to the technical system, i.e.: '*Technical identity systems must only reveal information identifying a user with the user's consent.*'[23] He has adopted this goal because he believes there are tendencies that

[19] Hughie Mackay and Gareth Gillespie. "Extending the social shaping of technology apprach: ideology and appropriation." (*Social Studies of Science 22,* 1992): 685–716. – Nelly Oudshoorn and Trevor Pinch, *How users matter: the co-construction of users and technologies*. London. (London University Press, 2003).

[20] Lotte Vermeir, Tim Van Lier, Jo Pierson and Bram Lievens, "Making the online complementary to the offline: social requirements to foster the 'sens of community" Paper presented at IAMCR conference, Sweden, 2008.

[21] Ann Cavoukian, "Privacy by Design."

[22] Tom Olzak, "Unified Identity Mangement", (InfosecWriter, 2006).

[23] Kim Cameron, "The laws of identity", Kim Cameron's Identity Weblog.

will '*erode public trust in the Internet*.'[24] This would threaten the possible positive future of the Internet. The corrosion of trust inherent in the web of the 90s: '*The Internet was built without a way to know who and what you are connecting to. This limits what we can do with it and exposes us to growing dangers.*'[25]

The same aspect of not knowing to whom or what a user is connecting is also apparent on SNS. With regard to SNS, we want to see an answer to this question of connection, because we expect that users are unable to fully perceive to whom they are connecting. This issue causes privacy and trust problems, which are one of the biggest forms of trust erosion on social media. We therefore wish to reinvestigate the seven laws of identity for privacy on social media. We believe that these laws may comprise liberating affordances for the Internet, especially in an age of mass self-communication. The seven laws of identity are the following.[26]

Law 1: User control and consent
'*Technical identity systems must only reveal information identifying a user with the user's consent.*' The individual is regarded as the most important part of the identity metasystem. The technology must be in control of the user and not the other way around. Moreover the technology should protect the user from deception, e.g. phishing.

Law 2: Minimal disclosure for a constrained use
'*The solution which disclosues the least amount of identifying information and best limits its use is the most stable long term solution.*' A breach is always possible. Therefore a 'need to know' basis of the identity metasystem is preferred. Cameron gives the example of 'age category' being different from 'birth date'. '*If a scenario requires proof of being a certain age, then it is better to acquire and store the age category rather than the birth date. Date of birth is more likely, in association with other claims, to uniquely identify a subject, and so represents "more identyfying information" which should be avoided if it is not needed.*'

Law 3: Justifiable parties
'*Digital identity systems must be designed so the disclosure of identifying information is limited to parties having necessary and justifiable place in a given identity relationship.*' The user must understand with whom information is being shared. Infocards a Windows identity Metasystem integrated in Internet Explorer 7 is a clear operationalization of this notion.[27] Windows designed a metasystem in which users can decide how much information they disclose to whom on the Internet through a standardised system. This system has many similarities to Facebook's identity system.

[24] Kim Cameron, "Laws of identity."

[25] Kim Cameron, "Laws of identity."

[26] The seven laws presented here are entirely based on the document of Kim Cameron "Laws of identity."

[27] Tom Olzak, "Unified Identity Management"

Law 4: Directed identity
'*A universal identity system must support both "omni-directional" identifiers for use by public entities and "unidirectional" identifiers for use by private entities thus facilitating discovery while preventing unnecessary release of correlation handles.*' Identity is regarded as always being directed to someone, where a distinction is made between private and public entities. According to Cameron Bluetooth is a technology that does not yet conform to the fourth law, because public beacons are used for private purposes.

Law 5: Pluralism of operators and technologies
'*A universal identity system must channel and enable the inter-working of multiple identity technologies run by multiple identity providers.*' Different parties should manage the digital identity as providing different features in each context. There is no such thing as one identity and one context in which the identity can be announced. Hence, many people would not want government identifiers to control their private identity.

Law 6: Human integration
'*The universal identity metasystem must define the human user to be a component of the distributed system integrated through unambiguous human-machine communication mechanisms offering protection against identity attacks.*' Not only control by the user is important. The technology should also integrate the human as part of the technology in order that the technology is adjusted to the capabilities of the user. Plain language is thus key.

Law 7: Consistent experience across contexts
'*The unifying metasystem must guarantee its users a simple consistent experience while enabling separation of contexts through multiple operators and technologies.*' Identities should be grasped as "things" that can be composed by the user. Moreover, they should have the freedom and liberty to choose when a certain thing is displayed and when not. On the other hand '*these options need to be consistent and clear. Consistency across context is required to be done in a way that communicates unambiguously with the human system components.*'

We consider each of the above-formulated laws as important in developing an identity metasystem. There is however room for improvement. Section 11.3 will describe some initial social requirements of SNS and Sect. 11.4 will combine existing literature with these social requirements to develop four identity claims that could adjust and optimize the seven laws of identity.

11.3 Initial Social Requirements of SNS

In describing the initial social requirements, which have initially been worked out, we will differentiate between the social requirements of identity processes and the social requirements of privacy issues. The first set on requirements focusses on the

needs and advantages of announcing the identity on SNS, intertwined with contextual privacy problems. The second set of requirements focus on what users want and need in protecting their privacy on SNS. We have separated these requirements because they cannot be reduced to each other, e.g. a teacher may announce herself as a good-looking single, open for relationships on a SNS (identity requirement), but she may want to keep this from her students (privacy requirement). We should emphasize that the social requirements will be only briefly discussed here. For a more elaborate view on these requirements and the theoretical and methodological background reference is made previous work by De Wolf and Pierson discussing the Symbolic Interactionist perspective on linking privacy and identity on social network sites.[28] For the purposes of this paper it suffices to say that 15 adolescents between the age of 14 and 18 were interviewed regarding their online behaviour on Facebook and Smartschool (a Belgian digital learning platform). All interviews were obtained in June and July 2011 in Flanders (the Northern part of Belgium) and took place in a public setting like a library or a pub. The focus is on how an online self on SNS is acquired and how this interconnects with the context problems of privacy. To pin down the relationship between identity and privacy the theoretical framework of Symbolic Interactionism combined with a qualitative ethnographic study was used.

11.3.1 Social Requirements of Identity

If SNS are compared to an offline environment, important differences can be observed. Specifically, everything in offline environments is situated in a certain context and most of the time we know what roles we ought to perform, which things can(not) be said, who is present and watching our behaviours and what relationships we have with whom. On SNS we have a lack of a clear definition in time and space. We are not sure who is watching our behaviour.[29] We are confronted with context collision,[30] a blurring between private and public,[31] invisible audiences[32] and forced disclosure.[33]

---

[28] Ralf De Wolf and Jo Pierson, "'Symbolic Interactionist perspective on linking privacy and identity on social network sites" Congres paper for ICA 2012. (Submitted)

[29] With this problem we refer to the fact that people often do not know what happens with their personally identifiable information (PII), with questions like, 'who gathers it?' and 'why do they gather it?' – Daniel Solove, "Privacy and power: computer databases and metaphors for information privacy", (*Stanford law review 53*, 2001),1393.

[30] With context collision we refer to the collapsing or blurring of different contexts online – Danah Boyd, "Taken out of context."

[31] Danah Boyd, "Taken out of context."

[32] Danah Boyd, "Taken out of context."

[33] Forced disclosure refers to the ongoing process of clarifying private information through private information. A problem, combined with context collison that can cause annoying problems for the user – Jeffrey Rosen, "Out of context: the purposes of privacy." (*Social Research* 68, 2001): 209–222.

On the one hand, all of these issues seem like privacy invasive elements. On the other hand, these elements seem to have a positive influence on many identity processes among the adolescent population. In this section four important so-called social requirements of identity are briefly explained.

1. A first social requirement of identity emphasizes the possibility announcing the own identity in ways that are easier, less direct, complementary and new in comparison to an offline environment. In previous work we found that the process of announcements, that is presenting the own identity to the outside world, is facilitated when there are no clear boundaries in the context in which one is acting. For example, it is easier to change your relationship status on Facebook from 'in a relationship with' to 'single' than to explain it over and over again in the offline world to different groups of people.
2. Moreover it seems that filling up this fuzzy context environment of SNS with meaning is empowering and liberating for the user. For example, Facebook is also used as an outlet for frustrations when nobody is around or direct conversation is perceived as undesirable.
3. Not only announcements but also placements,[34] that is the acknowledgement and placing of the other in the identity that is being announced, seem to be facilitated. For example, the like-button was perceived as a useful tool to easily place one another.
4. Last but not least the process of altercasting seems to be modified on SNS. Altercasting can be defined as '*the social process in which a person's acts constrain and shape acts of another by "casting" the other into a role of the altercaster's choosing*', thus Hewitt.[35] It is often difficult to define the relationship one has with others. Facebook was used as a tool to make these relationships more clear and prominent. For example, tagging other people in your own profile picture with the inscriptions like 'best friends'.

It is our task as social scientists to take into account these positive features of SNS when developing privacy enhancing technologies. Otherwise there is the possibility of harming the identity layer and uniqueness of announcing the identity on SNS.

11.3.2 Social Requirements of Privacy

In grasping the behaviours of adolescents on SNS it is important to know how exactly they interpret the privacy problems defined in the literature. Context collision[36]

[34] These concepts are used within the framework of Symbolic Interaction and can be seen as two sides of the same coin in identity formation. The former is everything a person does to bind himself with a specific identity. The latter is the reaction of others in confirming the announced identity.

[35] John Hewitt, Self and Society: a symbolic interactionist social psychology (10th ed.). (Boston Mass.: Allyn and Bacon, 2007), 167.

[36] Danah boyd, "Taken out of context."

or context collapse[37] refers to the blurring of context in the online environment, whereas in an offline environment more or less strict barriers can be distinguished. This blurring of contexts can make it hard for people to represent themselves to multiple audiences in one space and time. We found that adolescents did not perceive this as a social privacy problem.

1. However active context collision by certain segments on SNS was found privacy intrusive. The presence of different contexts *an sich* was not defined as a problem. For example, the most of our respondents had parents or other family members in their list of friends on their Facebook account. But this was not perceived as a problem, unless they started meddling with their private life for example by commenting on pictures of them with their friends. Next to this we found that the 'generalized others' on Facebook were rather weak. The generalized others '*is best thought of as the imagined perspective of an imagined other, whether this is the whole society, the community to which the individual belongs, or some smaller category of grouping of people*', according to Hewitt.[38] It is difficult to know who 'Facebook' is and what it exactly does. Moreover, this platform is not questioned because everyone else is using it. This leads us to the next three social requirements of privacy.
2. Making the 'real' generalized others of Facebook much more transparant. With this we mean that the user ought to become aware of who or what Facebook is, namely an American company organisation looking over your shoulder and pushing you to disclose personal identifiable information (PII) for commercial purposes. Personal identifiable information or PII is not only limited to directly identifiable information such as a user's name. PII can also be information that can only partly identify a user. The combination of date of birth and hometown may identify someone, but without linking these two it is impossible to single out one person. PII is used to stress that age, hometown and other partly identifying information should not be seen as anonymous information although companies such as Facebook often describe it as such.
3. Institutionalizing the generalized others of existing offline communities online, without touching upon the unique identity features. When comparing Facebook with Smartschool[39] we found that the generalized others (of the school) of the latter was very present and influenced the behaviour of the respondents. The last thing we want is a 'big brother' on Facebook. That would only deprive the user in writing the identity into being online. Here we see how identity requirements can be at odds with privacy requirements. Then again, the user has the right to know what exactly Facebook is doing with their PII. However, generalized others could also be established differently on SNS, without the 'big brother effect' and without referring to the 'real intentions of Facebook's generalized others'. Institutionalizing

[37] Jeffery Rosen, "Out of context."

[38] John Hewitt, Self and society, 75.

[39] Smartschool is a commercial digital learning environment (DLE) owned by Smartbit in Belgium.

Table 11.1 Initial social requirements of SNS

Social requirements of identity processes
(a) Possibility of announcing the own identity in ways that are easier, less direct, complementary and new in comparison to an offline environment
(b) Possibility of filling up the fuzzy context environment
(c) Possibility of altercasting another individual
(d) Possibility of easily placing another person in his or her announced identity
Social requirements of privacy issues
(a) Discouraging active context collision by certain segments on SNS
(b) Making the 'real' generalized others of Facebook much more explicit
(c) Institutionalizing the generalized others of offline communities online, without touching upon the identity layer
(d) Stimulating the process of deindividuation in order to stimulate privacy behaviours.

the generalized others of communities of interest the users are involved with offline could also influence their behaviour without being depriving.

4. Stimulating the process of deindividuation in order to stimulate privacy behaviours on SNS. The remark 'everybody else is using the platform, so why shouldn't I' was a phrase that was often heard during the interviews. It seems like the respondents are immersed in the mass and in that way feel invulnerable. Reversing this process of deindividuation in order to make the user responsible for her actions on SNS could be of value in developing privacy enhancing technologies. The table below summarizes the different social requirements of identity and privacy (Table 11.1).

11.4 Identity Claims

In this section we will bundle the previous section on social requirements together with identity and community literature on SNS to compose four identity claims. (1) Offline and online communities are intertwined but not the same, (2) personal information on (the Internet) is networked, (3) individuals are often unaware of their identity processes and (4) privacy, identity and capitalism are interconnected. On the basis of these four claims we would like to update the seven laws of identity into a useful tool in the process of requirement engineering.

11.4.1 First Identity Claim: 'Offline and Online Communities are Intertwined but Not the Same'

'Community' is an old concept and often contested in its nature. It is beyond the scope of this paper to elaborate on all the different views of community in present society, but in order to prove the previously mentioned identity claim, the view of

Rheingold on online communities seems a good starting point. Rheingold[40] can be seen as the first author to use the concept of virtual communities. His thoughts should be captured in the spirit of time. That is when the Internet began to bloom in the consciousness of the public.[41] With his concept of virtual communities he refers to a non-existant offline community, solely rooted in cyberspace. '*What is significant about his view on virtual communities is that virtual communities are 'communities on the Net'. They do not exist in everyday life*', according to Delanty.[42] Even further, the downfall of communities in real life could be compensated by a virtual one. It is clear that his view on the Internet is out-dated and a more interactionist view on reality and the virtual is necessary. There is still a lot of discussion on the place and meaning of (online) communities in present society,[43] but studies have revealed a clear connection between offline and online environment. In studying Facebook Lampe et al.[44] found that it is used primarily for maintaining previous, offline relationships. When conducting research on MySpace boyd and Ellison[45] found that teenagers are motivated to go on SNS because their offline friends are there too. According to boyd,[46] Friendster too is deeply connected to the participant's offline social life. Miller and Slater[47] state that almost always online and offline spheres are interconnected, through which one reality is created. When studying MySpace, Parks[48] found that '*offline and online communities are linked in ways that we are only beginning to understand.*' Moreover, he states that '*…it may be more accurate to say that virtual communities are often simply the online extension of geographically situated offline communities.*' According to recent data from Pew research centre[49] only a small fraction of friends people they have on Facebook are people we have never met offline. Eighty-nine percent of the friends a user has on Facebook have been met more than once offline. Hence, we could state that offline and online communities are clearly intertwined.

---

[40] Howard Rheingold. *The virtual community: homesteading on the electric frontier*. (USA: MIT Press, 2000).

[41] Malcom Parks, "Social network sites as virtual communities" in *A networked self: identity, community and culture on social network sites*, ed. Zizi Paparachissi (New York and London, Routledge, 2011).

[42] Gerard Delanty, *Community*, (London and New York, Routledge, 2003).

[43] Zygmunt Bauman. "Identity in the globalizing world." In *Identity in question*, ed. Anthony Elliot and Paul du Gay (Sage publications, 2008). – Gerard Delanty, *Community* – Craig Calhoun, "Community without propinquity revisited: communications technology and the transformation of the urban public sphere", *Sociological inquiry 68* (1998): 373–397.

[44] Cliff Lampe et al., "a face(book) in the crowd." Paper presented at the 2006 20th anniversary conference on Computer supported cooperative work – CSCW, Canada, 2006.

[45] Danah boyd and Nicole Ellison, "social network sites: Definiton, history, and scholarship", *Journal Computer-Mediated Communication 13* (2007).

[46] Danah boyd, "Friends, friendster, and myspace top 8: writing community into being on social network sites", *First Monday 11* (2006).

[47] Daniel Miller and Don Slater, *The Internet: An Ethnographic Approach*, (London: UK: Berg, 2000).

[48] Malcom Parks, "Social network sites."

[49] "Pew Internet and American Life Project."

However, this is only a segment of our first identity claim. We also want to prove that the offline and online world differ quite substantially. We will start by elaborating upon a concept of Zhao et al.,[50] namely 'hoped-for-possible selves'. Zhao et al. state that the way people profile themselves in an offline environment differs considerably from an online environment, which can exert positive influences on the self-image and esteem. So they conceive identity construction as different in a *nonymous*[51] online world (e.g. Facebook) versus a nonymous offline world. A nonymous environment refers to an online context in which the offline identity is displayed. He uses the term nonymous to contrast with an anonymous online environment, in which people do not have to display their offline identity, e.g. online dating site match.com. Consequently, there does not have to be a connection to the offline world in the latter. In a nonymous online environment people have to display their offline identity, but have control over how it is displayed. It looks like people take advantage of this opportunity to '*stretch the truth a bit, for creating their hoped-for-possible-selves*', as Zhao et al. would say. De Wolf and Pierson[52] investigated how the online self is acquired on SNS and found that identity processes are perceived differently than in an offline world. '*Behaviour on Facebook can be seen like a performance on stage. The respondents – usually – did not want to profile themselves to just one person or segment. They wanted to announce their own identity to the world*', according to De Wolf and Pierson.[53] This kind of interpretation of identity processes online leaves room for behaviour that otherwise would not be performed in the offline world. In a previous sect. (11.3.2) we described these behaviours as social requirements of identity on SNS.

11.4.2 Second Identity Claim: 'Information (on the Internet) Is Networked'

On the topic of privacy online, boyd[54] stated recently '*that the solution to this puzzle will not be to restrict data collection or to enhance individual control over specific items of data, but to think long and hard about what happens as the data flows across networks and as the data is networked together. This requires moving beyond the individual and focussing on the collective*'. Like boyd we think that we need to focus beyond the individual control over data. Moreover, it seems necessary to mitigate the responsibilization of the individual in this process. In this section we will use the

[50] Shanyang Zhao et. al., "Identity construction on facebook: Digital empowerment in achored relationships", *Computers in Human behaviour 24* (2008): 1816–1836.

[51] The concept of nonymous is used to constrast with anonymous.

[52] Ralf De Wolf and Jo Pierson, "'Symbolic Interactionist perspective."

[53] Ralf De Wolf and Jo Pierson, "'Symbolic Interactionist perspective."

[54] Danah boyd, "Networked privacy", http://www.danah.org/papers/talks/2011/PDF2011.html.

Symbolic Interactionist (SI)[55] view to elaborate how the self is socially constructed and how everything about information is networked in an online and offline world.

According to SI, it is the act of speech that is an essential factor for the evolutionary development of human consciousness. Hewitt[56] states that this factor has three consequences for human life: (a) It transforms the environment people live in, because we can manipulate the environment and transform it from relative concrete to more or less abstract; (b) the possibility to displace oneself into the other, by which shared meaning can be established and; (c) the individual can become part of the environment. If individuals can designate the environment through symbols, it is also possible in designating oneself as an object as well as being acted upon. We think that this latter fact is often over-emphasized, whereas the accent should be on 'interaction' and not on the 'individual'.

There are a lot of different factors that an individual has to take into account in order to coincide the own behaviour with that of the situation and others: what role should be performed, what content could be brought up, how content ought to be brought up, etc. If we were to grasp this on a more abstract level we could ask ourselves why we always put the individual into the centre of attention in identity formation that is socially constructed. Other factors seem to be equally important. Of course, having an individualistic view on the user is not a problem as long as the different structures, in which one is acting, are adequate and not questioned. It is only when all of this fails, that the negligible role of the individual becomes clear. This is exactly what we see happening on the topic of privacy issues on SNS.

Interactions on SNS – as well as on any other technology aiming at social interaction – are a simulation of real life conduct.[57] Whereas in an offline setting a more or less clear definition of the situation in space and time can exist, an online setting does not guarantee this: who is watching our behaviour (space) and what happens with our information (time)? It seems that information is developing a story of its own, without being in control of the individual. To put it otherwise, information is becoming networked and very fluid, beyond the individual.

11.4.3 Third Identity Claim: 'Individuals Are Often Unaware of Their Identity Processes'

In the previous section we have elaborated our view on how information is always networked and how the role of the individual within this process is over-emphasized. In this section we want to build further on this insight to clarify our third claim on the unawareness of individuals of their identity formation on SNS.

---

[55] The Symbolic Interactionist School highlights the reciprocal relationship between the individual and the group it is embedded in. Moreover, it studies the way society is created through interaction.

[56] John Hewitt, Self and society, 40–44.

[57] Sherry Turkle, "*Alone together: why we expect more from technology and less from each other*", (New York: Basic Books, 2011).

MacKenzie and Wajcman[58] claim that technologies are always socially shaped and '*involve economic decisions made by complex social institutions operating over long periods.*' To illustrate this claim they have compared the evolution of the gas refrigerator with his electric rival. Eventually, the latter prevailed and is now considered as a given. On first sight we would think that the electric refrigerator was technologically better designed. However, this does not seem to be the case. Mackenzie and Wajcman[59] claim that '*we have compression, rather than absorption, refrigerators in the United States today not because one was technically better than the other, and not because consumers preferred one machine (in the abstract) over the other, but because General Electric, General Motors, Kelvinator and Westinghouse were very large, very powerful, very aggressive, and very resourceful companies, while Servel and SORCO were not.*' Today, it seems that nobody questions the existence of the electric refrigerator and the annoying humming it makes – which the gas refrigerator did not have, because it did not require a motor. Mackenzie and Wajcman[60] rightly indicate the negligible role the consumer played within this process: '*Consumer 'preference' can only be expressed for whatever it is, in fact, available for purchase, and is always tempered by the price and convenience of the goods that are so available.*' Without being economically deterministic we are also concerned about the 'gap of influence' between the consumer and the producer of goods. What we want to highlight here is the unconsciousness to which this process contributes: Without knowing that the refrigerator could have existed without its 'hum', can we question it? Without knowing that SNS providers collect PII and the interrelation between identity and privacy on SNS, can we question it?

Berger and Luckman stated that sociology should become '*an inquiry into the ways in which everyday ideas about reality are created and maintained.*'[61] Hence, they focused on the everyday construction of social reality. Berger[62] described a three way process on how the social reality comes to existence.

> Externalization (1) is the on-going outpouring of human being into the world, both in the physical and the mental activity of men. Objectivation (2) is the attainment by the products of this activity (…) of a reality that confronts its original producers as a facticity external to and other than themselves. Internalisation (3) is the reappropriation by men of this same reality, transforming it once again from structures of the objective world into structures of the subjective consciousness. It is through externalization that society is a human product. It is through objectivation that society becomes a reality sui generis. It is through internalization that man is a product of society.

---

[58] Donald MacKenzie and Judy Wajcman, *The social shaping of technology: how the refrigerator got its hum* (Open University Press, 1985): 1.

[59] Donald MacKenzie and Judy Wajcman, *The social shaping of technology, 9.*

[60] Donald MacKenzie and Judy Wajcman, *The social shaping of technology, 10.*

[61] Steven Seidman, *Contested Knowledge: social theory today 3th edition* (UK: Blackwell Publishing, 2004): 81.

[62] Peter Berger, *The Sacred Canopy: Elements of a Sociological theory of Religion* (New York: Anchor, 1967): 4.

Table 11.2 Process of construction of technology

Berger (1967)	Pinch and Bijker (1987)	Taken together…
Externalisation	Interpretative flexibility	Technology is a human product
Objectivation	Closure	Technology is taken for granted
Internalisation	Wider context	Man is a product of technology

We believe that this process describes well how social reality is constructed, taking into account both agency and structure elements. The social construction of technology (SCOT) describes a similar phasing, applied in the domain of technologies. SCOT, can be seen as part of the theoretical framework of social shaping of technology (SST).[63] In a first stage Pinch and Bijker[64] describe '*how technological artefacts are culturally constructed and interpreted.*' With this they try to clarify that there is not just one way of constructing technology and that meaning is poured into technology. In the second phase of 'closure' we observe a stabilization of technology and a disappearance of possible problems, where it is more important that the problem is not regarded as a problem, than a solution being found. In a last stage they refer to the wider context in which '*the sociocultural and political situation of a social group shapes its norms and values, which in turn influence the meaning given to an artefact* (Table 11.2).'[65]

What we find particularly interesting about the dialectic process of society shaping described by Berger[66] is how the relationship between objectivation and internalization is blurred and the '*socially produced institutional world is internalized by the individual, as an objective, natural order.*'[67] According to our results (3.1 and 3.2) the identity formation on SNS is not questioned or reflected upon enough. Most of the time people 'just do' and do not ask 'why' they are engaged in certain activities. People seem to be unaware of their identity processes online. This does not, howver, have to be solely excluded as a negative. We could state that this 'undergoing of structures' makes societal life easy and enjoyable. However, a certain amount of self-alienation[68] is necessary. Otherwise, we reduce ourselves to herd behaviour. Berger and Luckman call this process of herd behaviour 'reification' and it occurs '*when the institutional order is assumed to have taken on a life of its own independently of human intentions and needs.*'[69] This is a concept that is missing within the

[63] Robin Williams and David Edge, "the shaping of technology", Research policy 25 (1996): 865–899.

[64] Trevor Pinch and Wiebe Bijker, "The social construction of facts and artifacts: or how the sociology of science and the sociology of technology might benefit each other" in *the social construction of technology systems*, *ed.* W.E. Bijker, T. P. Hughes & T.J. Pinch. (1987): 40–48.

[65] Trevor Pinch and Wiebe Bijker, "The social construction of facts", 48.

[66] Peter Berger, *The Sacred Canopy, 4.*

[67] Steven Seidman, *Contested Knowledge, 83.*

[68] We define self-alienation as the process in which the individual looks at his own behaviour from a third person point of view. We do not denote this concept as solely negative nor positive. However a certain degree of self-alienation seems desirable.

[69] Steven Seidman, *Contested Knowledge, 83.*

framework of Pinch and Bijker. But the concept of self-alienation can be easily applied to the domain of SCOT.

In this section we would also like to denote the relation between alienation and empowerment, which is often overlooked. Empowerment is defined as something '*enabling people to control their own lives and to take advantage of opportunities.*'[70] The use of the notion of 'empowerment' is a long-standing tradition especially in the social welfare and radical education literature. When applying it in the analysis of the implications of communication technology, however, it is crucial to take into account Mansell's[71] critique on the discourse surrounding new media innovations that simply presumes users or citizens can reap the benefits of these innovations from the moment they are implemented. '*There is, therefore, a growing need to examine whether the deployment of new media is consistent with ensuring that the majority of citizens acquire the necessary capabilities for interpreting and acting upon a social world that is intensively mediated by the new media.*'[72] We should, however, also ask ourselves if empowering the user is always desirable. Empowering users of something they are not aware of automatically requires a certain degree of self-alienation, which could lead to depriving the user from expressing their identity online.

11.4.4 Fourth Identity Claim: 'Identity, Privacy and Capitalism Are Interconnected'

Identity, privacy and capitalism are connected but the strength of the tie between the different concepts depends on the way the user is being approached as a research object.

If the user is described as a research object that tries to use SNS as a means of forming an identity, than researchers are looking at the positive aspects of this process.[73] Castells uses social media as a clear example to show how users are empowered to communicate more easily with a larger audience. He calls this mass self-communication.[74] Although Castells recognized that the companies who own social media were curtailing these abilities, he still sees the user as a creative agent with unprecedented autonomy and new capabilities. As long as users are seen as actors, privacy issues are put forward as consequences of user behaviour.

---

[70] Laurent van der Maesen and Alan Walker, "Social quality: the theoretical state of affair", *European Foundation of Social Quality* (2002).

[71] Robin Mansell, "From digital divides to digital entitlements in knowledge societies", *Current sociology 50* (2002): 407–426.

[72] Robin Mansell, "From digital divides", 409.

[73] Danah Boyd, "Why youth (heart) social network sites: the role of networked publics in teenage social life"*, MacArthur Foundation Series on digital learning – youth, identity, and digital media 26* (2007).

[74] Manuel Castells, "communication power and couter-power in the network society", *International Journal of Communication 1* (2007): 238–266.

This privacy as a user responsibility is also visible in the following example. Weitzner et al.[75] put forward the scenario of a single mother, Alice. She is empowered to buy books online and joining several discussion boards on social media to inform herself and others about a disease her son has. This has negative consequences on her chances of finding a job since employers perform background checks before they accept candidates. These background checks are not only limited to the capabilities or the reputation of a candidate, they are also focused on finding financially risky candidates and eliminating them from the list.

Another school of thought looks at privacy, identity and capitalism from a neo-Marxist viewpoint. The user is no longer an agent but a number in a database. '*Negative approaches see surveillance as a form of systematic information gathering that is connected to domination, coercion, the threat of using violence or the actual use of violence in order to attain certain goals and accumulate power, in many cases against the will of those who are under surveillance*', according to Fuchs.[76] One of the main problems with this depiction is that it resembles the comic situation two pigs, located in a meat-processing factory, are very pleased with the fact that they get free housing and food. This is very problematic because users are not merely cattle that are given things for free just to kill them in the end. Users are more like clients of a pub. A pub with no one to meet is an uninteresting pub, but a pub that is filled with friends on Friday evening is worth visiting. The pub works in two ways, first it works as a place were friends can meet and secondly it is expected from you to buy a few drinks. This metaphor to illustrate the negligible role of the user on SNS is also lacking because users are not only inviting other users until a critical mass is reached and everyone wants to hang out in the most popular bar. Users are also creating content, uploading pictures and interacting with each other, but those things stay in the 'pub', which creates an extra reason to stay. Thrift[77] refers to this as 'knowing capitalism'. Once you are on an SNS, these platforms want the user to share information and stick to it.

Two approaches to social media can thus be separated. One in which the user is a producer of meaning and content, User Generated Content (UGC), which can be placed in the larger context of mass self-communication. The privacy as surveillance school depicts users as being subject to a panoptic sorting machine in which they are all stripped of their subjectivities and motivations to participate in this malicious top-down machine. This machine needs Personal Identifiable Information to organize audiences into groups, which serve to accumulate some kind of power. User Generated Content is used to attract and entertain users while the same content may also be used as PII to organize users as audiences which show a bigger chance of being interested in certain advertisements and products. We keep both terms because they signify the difference between two different logics or privacy discourses.

---

[75] Daniel Weitzner, "Information accountability", *Communication of the ACM 51* (2008): 82–87.

[76] Christian Fuchs, "New Media, Web 2.0 and Surveillance", *Sociology Compass 5* (2011): 134–147.

[77] Nigel Thrift, *Knowing capitalism,* (New Delhi: Sage Publications, 2005).

Fig 11.1 Example of social advertising on facebook

In contemporary SNS these two logics of privacy are intertwined into what has been called social advertising. This can be defined as a particular form of targeted advertising wherein the advertised product is endorsed by a user to another targeted user. The endorsing aspect is achieved through UGC because the advertisement itself is shown as a story, which is sometimes indiscernible from other UGC. This intertwinement of UGC and targeted advertising is not new. In fact we can find three different ways in which this intertwinement generates value for social media companies. Cohen,[78] Coté and Pybus[79] have already pointed out that the UGC provided on social media works as glue, which motivates users to stay logged in and interested in a particular social media platform. This factor of returning and staying on a platform is called 'stickiness'. This stickiness is a means to create more eyeballs, which can be translated into direct economic value.[80] Secondly, UGC is also used as PII to profile users into segments of users who are more apt to be interested in the advertised product or service, which makes them sellable as a distinct audience.

We have found a third and new way of commodifying these subjectivities. Social advertising uses the interpersonal relationships between users as an extra meaning. This meaning is incorporated in the message. This form of advertising consists out of the following steps. (1) A user starts following a brand of product on Facebook by liking it. (2) Facebook publishes this story as a normal event. (3) If a company pays for this story to be shown more, it can be shown as a sponsored story to a specifically targeted audience. It is important to note that the audience must have a relationship with someone who has recently engaged the advertised brand (Fig. 11.1).

[78] Nicole Cohen, "the valorization of surveillance: Towards a political economy of Facebook", *Democratic Communiqué 22* (2008): 5–22.

[79] Mark Coté and Jennifer Pybus, "Learning to immaterial labour 2.0: MySpace and social networks", *Ephemera: Theory & Politics in Organization 7* (2007): 88–106.

[80] Nicole Cohen, "the valorization of surveillance."

Identity, privacy and capitalism are thus connected. This connection is not questioned in the work of Coté and Pybus who pointed out the two-sided aspect of UGC and PII wherein UGC was created to form an identity and PII to create value for a company: '*every time the user submits a search topic, it accretes – like surplus labour – in the Google database and in turn micro targets an advertisement tailored not only to that particular user but to that specific search*.'[81] We question this entwinement because the motivation of the initial announcement differs from the consequent generated announcement. In the first case, someone "likes" something as a social announcement, but in the third case, someone is shown as being part of an ad. Is this incorporation of UGC in advertising acceptable for users? Do they see a difference between the two announcements in terms of identity, privacy or even as being a part of a capitalist system?

11.4.5 Identity Claims Conclusion

The first identity claim of 'online and offline community being intertwined but not the same' teaches us that we can use the offline environment in tackling the privacy issues online: what can we learn of offline communities in enhancing privacy on SNS? We should, however, take into account that 'identity' and 'community' differ online and offline. To simply copy-paste offline regulations (e.g. partial identities, circles, smart lists) is denying the uniqueness of SNS. The second and third identity claim teaches us that a focusing soleley on the individual is not enough. We need to focus on the collective and move beyond the individual in preserving privacy on SNS. The third identity claim teaches us that we have to measure the awareness and behaviours of individuals and delineate the degree of self-alienation that is desirable. The fourth and final identity claim teaches us that we have a clear interconnection between privacy, identity and capitalism. Any privacy enhancing technology that is being developed should take this claim into account. Otherwise, technologies are being created in thin air. Moreover, a technology should consider a trade-off inherent in the design, in which self-deprivation seems necessary.

11.5 Seven Laws of Identity Revisited

In this section we will set the seven laws of identity of Cameron (Sect. 11.2.2). against the four identity claims (Sect. 11.4).

The first law of identity states that '*identity systems must only reveal information identifying a user with the user's consent*'. At first sight this seems like something

[81] Mark Coté and Jennifer Pybus, "Learning to immaterial labour 2.0."

that is self-evident. However, this is a necessary but in itself an insufficient condition. This notion creates a false consciousness, stating that an individual on his/her own can completely control his or her information flow. Moreover this contributes to the responsibilization of the user of something that is impossible to control alone. The first law of identity clearly clashes with the second and third identity claim.

The second law of identity requires that '*the identity metasystem has to disclose the least identifying information possible*'. Nowadays the processes of identity on Web 2.0 applications have become an aspect of everyday normal life. Hence, it seems rather normal that a lot of information is disclosed on SNS. We agree with placing limitations on the collection and use of personal information. But we want to rethink how this trade-off should be for users. Are users receiving enough information and choices to make a balanced decision? Is this information presented in a biased way that benefits the commercial goals of social media? The answer to this question is positive, SNS and other social media need to attract revenue and the most common source of revenue is through targeted advertising, which is enabled by default and impossible to turn off.

So, the question about the minimum amount of PII disclosure or usage is actually a secondary question to: 'should these platforms be maintained in an economic system where commodification of PII through targeted advertising is enabled by default or should we look for alternatives?' Distributed SNS are a possible alternative but are users willing to abandon the lives or profiles they have built up there?

The third law of identity states '*that identity systems must be designed so the disclosure of identifying information is limited to parties having a justifiable place in a given identity relationship.*' This law presumes that the identity relationship between two parties is always known and can be defined. In real life most of the time everything is contextualized and we know what conduct we can perform and ought to expect from others, but on SNS this seems not to be the case. Furthermore we should ask ourselves if it is justifiable for an identity relationship between people (privacy as subject) or between a user and a private corporation or government (privacy as object) to always be defined by the user. As presented in previous chapter on the social requirements of SNS we could see that when a clear definition of the situation is lacking, this can be liberating and empowering for users of SNS qua identity formation. Moreover, roles and contexts on SNS are very fluid and flexible, which makes a definition of relationships very hard, as discussed in the second identity claim. To summarize, identity relationships are difficult to define and can cause more harm than good for the user qua identity formation. Regarding privacy as a subject, where the user is considered an agent of her identity, this seems rather clear. Relationships between people are constantly changing. To focus upon roles of who has a justifiable place within these relationships and who does not, seems like a waste of effort. That is why we suggest focusing upon the information stream itself. Regarding privacy as object we are not quite sure on how to interpret this third law of identity. When clear roles can be defined in a relationship between a user and private organization, this third law of identity makes sense. However, this presumes that users know that they have the primary role of a 'product' on SNS instead of a 'customer'. This seems to clash with the third identity claim.

The fourth law of identity states that '*a universal metasystem must support both "omnidirectional" identifiers for use by public entities and "unidirectional" identifiers for use by private entities.*' Again this notion presumes that people can always differentiate between groups of people (see critique third identity law). Moreover this seems difficult when information is networked. In conclusion, this fourth identity law is difficult to obtain when confronted with unawareness and information that is being networked with others.

The fifth identity law states that '*a universal identity solution must utilize and enable the interoperation of multiple identity technologies run by multiple identity providers.*' Multiple identity providers also include the users themselves. We completely agree with this fifth identity law. However, as the second claim of identity states, information on the internet is and always will be networked. We think that it is important that identity technologies are run by multiple identity providers. But we find the controlling of PII by the user even more important. The idea of distributed SNS (compatibel with the idea that users control their PII) instead of commercial SNS is appealing. We ask ourselves, however, if it is a good thing that PII is distributed to dozens of servers? Does this make the control of PII easier? Furthermore, does every user want this kind of control?

The sixth identity law states '*that the identity metasystem must define the human user to be a component of the distributed system, integrated through unambiguous man machine communication mechanisms offering protection against identity attack.*' We have two side remarks on this sixth identity law. Firstly, certain technologies like SNS can no longer be seen as a just a 'tool' that is used, but as an extension of the human user. It seems as though this technology is completely internalised and perceived as a given in contemporary society. This latter fact of internalisation is often overseen by the unaware user: Does the individual question her interrelation with the technology that she is using? Does the individual ask if her identity formation is different because of the opportunities that SNS have to offer? This is not always the case. According to the third identity claim finding the right amount of self alientation seems necessary for people to make them aware of their identity formation and privacy gaps on SNS. However we should not over-exaggerate this. Otherwise this could lead to depriving the user of expressing her identity online, or even worse, create a moral panic. Secondly, it is important to make a distinction between the individual as an individual user of technology or to approach the individual as a social being in interaction with others and the community one lives in. We prefer the latter. With this we like to emphasis the need for social requirements beyond the classical individual person perspective, as the second claim describes.

The seventh and last identity claim states '*the identity metasystem must guarantee its users a simple, consistent experience while enabling separation of context through multiple operators and technologies.*' A simple and consistent experience is exactly the opposite of what we experience on SNS. We do not have simple and clearly defined contexts on these platforms. Moreover, we need to give the user freedom to fill these contexts with meaning. Hence, defining a simple and consistent experience, like what the users is used to in the offline world, is denying the uniqueness and agency of the user. Instead we should focus beyond the offline metaphors on

behaviour.[82] As stated in the first claim, the offline and online world are interconnected, but not the same.

11.6 Overall Conclusion

We clearly see a responsibilization of the individuals who use or are affected by social networking services. SNS are being developed and have grown immensely in their use. But privacy measures, both where the user is both subject and object, are regarded as secondary in the development of these new technologies.

In this paper we have proposed trying and reverse the process in which the notion of privacy is embedded in the technology that is being developed. We therefore operationalized the concept of PbD through the process of requirement engineering and identified initial social requirements of identity and privacy of SNS based on communication science research. A clear application area of PbD is that of privacy and identity, taking shape into seven laws of identity. These laws are a good starting point for requirement engineering on SNS but have shortcomings from a social science perspective. The social requirements taken together with other literature on the topic of identity, community and privacy have been merged to develop four identity claims: (1) offline and online communities are intertwined, but not the same; (2) information on the Internet is networked; (3) individuals are often unaware of their identity processes and (4) identity, privacy and capitalism are interconnected. Finally, we set the laws of identity against these claims in order to steer the engineering process.

With this study we aimed to emphasize the need for a social perspective in creating privacy enhancing technologies, to make sure that these are not created in thin air but anchored in the context in whcih they are used. Looking at the current affordances of SNS we make give three critiques, based on the revisited identity claims. First, all trade-off measures are focused on privacy as subject. Privacy as object, or the controlling of the user of what kind of product she wants to be in relation to the SNS provider, is mostly out of the question. The user's options are always limited to accepting or declining the application. Secondly, most of the privacy measures regarding privacy as a subject are very individualistic and ignore the fact that PII is strongly networked. Moreover, it lacks a sense of creativity to focus beyond the offline world, only making clearly defined contexts possible. Thirdly and lastly, SNS assumes that the user is aware of her both subject and object on SNS, which of course is not the case.

The (social) requirements of SNS as well as their current affordances will be more elaborated upon further. On the one hand we will focus on operationalizing the revisited identity laws and concretize them into technological requirements in the engineering process. On the other hand we will focus on the current privacy related affordances on social media and how these challenge users' expectations and control over their privacy.

[82] We want to make clear that in an online world there are different laws and regulations on how to act. To simply copy-paste offline regulations, as in presenting clearly defined barriers (e.g. partial identities, circles, smartlists) is denying the uniqueness of SNS.

References

Bauman, Zygmunt. 2008. Identity in the globalizing world. In *Identity in question*, ed. Elliot Anthony and Paul du Gay. London: Sage publications.

Berger, Peter. 1967. *The sacred canopy: Elements of a sociological theory of religion*. New York: Anchor.

Berger, Thomas, Maren Hartmann, Yves Punic, and Katie Ward. 2005. *Domestication of media and technology*, 255. Berkshire: Open University Press.

Boyd, Danah. 2006. Friends, friendster, and myspace top 8: Writing community into being on social network sites. *First Monday 11*. http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/1418/1336. Accessed 30 Nov 2012.

Boyd, Danah. 2007. Why youth (heart) social network sites: the role of networked publics in teenage social life. In *MacArthur Foundation Series on digital learning – youth, identity, and digital media*, ed. David Buckingham, 1–26. Cambridge, MA: MIT Press.

Boyd, Danah. 2008.Taken out of context: American teen sociality in networked publics. Ph.D. dissertation, University of California, San Diego.

Boyd, Danah. 2011 Networked privacy. http://www.danah.org/papers/talks/2011/PDF2011.html. Accessed 6 June 2011.

Boyd, Danah and Hargittai Eszter. 2010.Facebook privacy settings: Who cares? *First Monday 15*. http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/viewArticle/3086/2589. Accessed 30 Nov 2011.

Boyd, Danah, and Nicole Ellison. 2007. Social network sites: Definition, history, and scholarship. *Journal Computer-Mediated Communication* 13: 210–230.

Calhoun, Craig. 1998. Community without propinquity revisited: Communications technology and the transformation of the urban public sphere. *Sociological Inquiry* 68: 373–397.

Cameron, Kim Blog. 2011. The laws of identity. Retrieved 17 Nov 2011, from: http://www.identityblog.com/stories/2004/12/09/thelaws.html.

Castells, Manuel. 2007. Communication power and couter-power in the network society. *International Journal of Communication* 1: 238–266.

Castells, Manuel. 2009. *Communication power*. Oxford: Oxford University Press.

Cavoukian, Ann. 2009. *Privacy by design: Take the challenge*. Toronto: Information and Privacy Commissioner of Ontario.

Cliff, Lampe, Ellison, Nicole and Steinfield Charles. 2006. A face(book) in the crowd. Paper presented at the 2006 *20th anniversary conference on computer supported cooperative work – CSCW*, Banff.

Cohen, Nicole. 2008. The valorization of surveillance: Towards a political economy of facebook. *Democratic Communiqué* 22: 5–22.

Coté, Mark, and Jennifer Pybus. 2007. Learning to immaterial labour 2.0: MySpace and social networks. *Ephemera: Theory and Politics in Organization* 7: 88–106.

De Wolf, Ralf, and Pierson Jo. 2012. Symbolic interactionist perspective on linking privacy and identity on social network sites. Congres paper for *ICA*, Phoenix (work in progress).

Delanty, Gerard. 2003. *Community*. London/New York: Routledge.

Deuze, Mark. 2011. Media life. *Media, Culture and Society* 33: 137–48.

Digimeter. 2008. Digimeter. http://digimeter.be. Accessed 19 July 2008.

Gürses, Seda, Carmela, Troncoso, and Claudia Diaz. 2011. Engineering privacy by design. Paper presented at the *annual CPDP conference*, Brussels, 29–30 Jan 2011.

Hewitt, John. 2007. *Self and society: A symbolic interactionist social psychology*, 10th ed. Boston: Allyn and Bacon.

Mackay, Hughie, and Gareth Gillespie. 1992. Extending the social shaping of technology apprach: Ideology and appropriation. *Social Studies of Science* 22: 685–716.

MacKenzie, Donald, and Judy Wajcman. 1985. *The social shaping of technology: How the refrigerator got its hum*. Philadelphia: Open University Press.

Mansell, Robin. 2002. From digital divides to digital entitlements in knowledge societies. *Current Sociology* 50: 407–426.

Miller, Daniel, and Don Slater. 2000. *The internet: An ethnographic approach*. London: Berg.

Olzak, Tom. 2006. Unified identity management. http://www.infosecwriters.com/text_resources/pdf/Unified_Identity_Management_TOlzak.pdf. Accessed 6 Nov 2012.

Oudshoorn, Nelly, and Trevor Pinch. 2003. *How user matter: The co-construction of users and technologies*. London: London University Press.

Parks, Malcom. 2011. Social network sites as virtual communities. In *A networked self: Identity, community and culture on social network sites*, ed. Zizi Paparachissi. New York/London: Routledge.

Pew. Pew internet and American life project. http://www.pewinternet.org/Reports/2011/Technology-and-social-networks/Summary.aspx.

PewInternet and American Life Project. Why americans use social media. Last modified on 15 Nov 2011. http://pewinternet.org/Reports/2011/Why-Americans-Use-Social-Media/Main-report.aspx.

Pinch, Trevor, and Bijker Wiebe. 1987. The social construction of facts and artifacts: or how the sociology of science and the sociology of technology might benefit each other. In *The social construction of technology systems*, ed. W.E. Bijker, T. P. Hughes, and T. J. Pinch, 40–48. Cambridge, Massachusetss: The MIT Press.

Raynes-Goldie, Kate. 2010. Aliases, creeping, and wall cleaning: Undertanding privacy in the age of facebook. *First Monday 15*. http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/viewArticle/2775/2432. Accessed 30 Nov 2011.

Rheingold, Howard. 2000. *The virtual community: Homesteading on the electric frontier*. Cambridge, MA: MIT Press.

Rosen, Jeffrey. 2001. Out of context: The purposes of privacy. *Social Research* 68: 209–222.

Seidman, Steven. 2004. *Contested knowledge: Social theory today*, 3rd ed. Malden: Blackwell Publishing.

Silverstone, Roger, and Leslie Haddon. 1996. Design and domestication of infomration and communication technologies: Technical change and everyday life. In *Communication by design: The politics of information and communication technologies*, ed. Robin Mansell and Roger Silverstone, 44–47. Oxford: Oxford University Press.

Smit, Wim, and Ellen Van Oost. 1999. *De Wederzijds beïnvloeding van technologie en maatschappij – een technology assessment-benadering*. Bussum: Uitgeverij Coutinho.

Solove, Daniel. 2001. Privacy and power: Computer databases and metaphors for information privacy. *Stanford Law Review* 53: 1393.

Thrift, Nigel. 2005. *Knowing capitalism*. New Delhi: Sage Publications.

Turkle, Sherry. 2011. *Alone together: Why we expect more from technology and less from each other*. New York: Basic Books.

Van De Broeck, Wendy. 2011. From analogue to digital: The silent (r)evolution? A qualitative study on the domestication of interactive digital television in flanders. Ph.D. dissertation, Free University of Brussels, Brussels.

Van der Maesen Laurent, and Walker Alan. 2002. Social quality: The theoretical state of affair. *European Foundation of Social Quality*.

Vermeir, Lotte, Van Lier, Tim, Pierson, Jo, and Lievens, Bram. 2008. Making the online complementary to the offline: Social requirements to foster the 'sens of community'. Paper presented at *IAMCR conference*, Stockholm.

Weitzner, Daniel. 2008. Information accountability. *Communication of the ACM* 51: 82–87.

Williams, Robin, and David Edge. 1996. The shaping of technology. *Research Policy* 25: 865–899.

Zhao, Shanyang, Sherri Grasmuck, and Jason Martin. 2008. Identity construction on facebook: Digital empowerment in achored relationships. *Computers in Human behaviour* 24: 1816–1836.

Part IV
Surveillance, Profiling and Smart Metering

Chapter 12
Smart Metering and Privacy in Europe: Lessons from the Dutch Case

Colette Cuijpers and Bert-Jaap Koops

12.1 Introduction

In 2009, the European Union enacted the Electricity Directive and the Natural Gas Directive.[1] These directives recommend the implementation of smart metering systems, in order to promote energy efficiency and to help consumers in saving energy. If an economic assessment of the long-term costs and benefits to the markets and the individual consumers is positive, the Electricity Directive stipulates that at least 80% of consumers shall be equipped with smart meters by the year 2020.[2]

The foreseen smart metering system has several functionalities, which are well captured in the following description:

> a new generation of advanced and intelligent metering devices which have the ability to record the energy consumption of a particular measuring point in intervals of fifteen minutes or even less; communicate and transfer the information recorded in real time or at least on a daily basis by means of any communications network to the utility company; enable a two-way communication between the meter and the central system of the utility company, the so called distribution systems operator (DSO) allowing for remotely control functionalities of the meter such as switch off from the delivery of energy.[3]

[1] Directive 2009/72/EC of the European Parliament and of the Council of 13 July 2009 concerning common rules for the internal market in electricity and repealing Directive 2003/54/EC, OJ 14.08.2009, L211/55. Directive 2009/73/EC of the European Parliament and of the Council of 13 July 2009 concerning common rules for the internal market in natural gas and repealing Directive 2003/55/EC, OJ 14.08.2009, L211/94.

[2] Directive 2009/72/EC, Annex I, art. 2.

[3] Rainer Knyrim and Gerald Trieb, "Smart metering under EU Data Protection Law", *International Data Privacy Law*, March 1, 2011, p. 121.

C. Cuijpers (✉) • B.-J. Koops
Tilburg Institute for Law, Technology, and Society (TILT), Tilburg University, Tilburg, The Netherlands

FRW-TILT, Tilburg University, 2, Warandelaan, P.O. Box 90153, 5000LE, Tilburg, The Netherlands
e-mail: cuijpers@tilburguniversity.edu; e.j.koops@tilburguniversity.edu

S. Gutwirth et al. (eds.), *European Data Protection: Coming of Age*,
DOI 10.1007/978-94-007-5170-5_12, © Springer Science+Business Media Dordrecht 2013

The implementation of smart metering at national levels can come in conflict with the legal framework regarding privacy and data protection. Energy consumption reveals details of personal life, in the most privacy-sensitive place – the home, and therefore smart metering has to strike a careful balance between detailed energy metering and privacy protection. A relevant case in point is the Netherlands, where in 2009, the First Chamber rejected two Smart Metering Bills because of privacy concerns, significantly delaying the large-scale introduction of smart metering. The Dutch case shows that a privacy impact assessment is vital for the introduction of smart metering.

In this paper, we present the recent developments in smart metering and describe the Dutch case, in order to draw lessons about assessing privacy compliance for countries that want to introduce smart metering.

We will start in Sect. 12.2 with a sketch of developments in smart grids and smart metering, as well as of the European legal framework regarding privacy and data protection. Next, in Sect. 12.3, we present the Dutch case of smart metering, analyzing the privacy aspects of the first smart metering Bill that was rejected by the First Chamber and of the repair legislation that was subsequently adopted. We pay particular attention to a report that put the initial smart metering Bill to the privacy test of Article 8 of the European Convention of Human Rights (ECHR). Based on the Dutch case, we conclude in Sect. 12.4 with a framework that can be used to assess the privacy implications of smart metering implementation.

12.2 Background

12.2.1 Smart Grids and Smart Metering

> Smart grids have an essential role in the process of transforming the functionality of the present electricity transmission and distribution grids so that they are able to provide a user-oriented service, supporting the achievement of the 20/20/20 targets and guaranteeing high security, quality and economic efficiency of electricity supply in a market environment.[4]

In 2009, the European Commission set up a Task Force Smart Grids to lay the foundations for smart grids in Europe. Its task is to identify and procure a set of regulatory recommendations to ensure EU-wide consistent and fast implementation of smart grids, while achieving all expected services and benefits for users.[5] The Task Force consists of three Expert Groups, of which the first (EG1) will identify

[4] Task Force Smart Grids, Expert Group 1 (EG1), *Functionalities of smart grids and smart meters*, December 2010, p. 4. http://ec.europa.eu/energy/gas_electricity/smartgrids/doc/expert_group1.pdf.

[5] Knyrim and Trieb, p. 127.

functionalities of smart grids and smart meters. In their final report, a smart grid is defined as:

> an electricity network that can cost efficiently integrate the behaviour and actions of all users connected to it – generators, consumers and those that do both – in order to ensure economically efficient, sustainable power system with low losses and high levels of quality and security of supply and safety.[6]

In contrast to traditional electricity networks, smart grids facilitate two-way energy traffic, enabling consumers with energy generators such as solar panels to transfer excess energy to the grid. Smart grids encompass a much wider area than smart metering, but smart metering is an important first step towards a smart grid as they "bring intelligence to the 'last mile' between the grid and the final customer".[7] EG1 even states that without this key element, the full potential of a smart grid will not be realized.[8] The two-way energy traffic requires two-way communication with the grid both for billing purposes and for optimising energy efficiency. Another key functionality of smart meters is that they provide detailed feedback to consumers on their energy consumption, which raises awareness and should incite them to save energy where possible.

Smart metering standardization is covered by a specific Mandate (M/441) by the Commission to the European Standardization Organisations (ESOs).[9] The work within the M/441 Mandate is overseen by the Smart Meters Co-ordination Group (SMCG).[10] The general objective of this mandate is: "*To create European standards that will enable interoperability of utility meters (water, gas, electricity, heat) which can then improve the means by which customers' awareness of actual consumption can be raised in order to allow timely adaptation in their demands*".[11]

The legal framework regarding smart meters in Europe can be described as an on-going process. The obligation to provide individual meters to end users was prescribed in Directive 2006/32/EC on energy efficiency.[12] This Directive is the

---

[6] Task Force Smart Grids, Expert Group 1 (EG1), p. 6.

[7] Idem, p. 16.

[8] Idem.

[9] Standardization mandates can be retrieved from: http://ec.europa.eu/enterprise/standards_policy/mandates/database/

The three standardization Mandates relevant in view of the Smart Grids Task Force are Mandate M/490 for Smart Grids (issued 1 March 2011), Mandate M/468 for electric vehicles (issued 4 June 2010) and Mandate M/441 for smart meters (issued 12 March 2009), http://ec.europa.eu/energy/gas_electricity/smartgrids/taskforce_en.htm.

[10] Task Force Smart Grids, Expert Group 1 (EG1), p. 5.

[11] Standardisation mandate to CEN, CENELEC and ETSI in the field of measuring instruments for the development of an open architecture for utility meters involving communication protocols enabling interoperability, p. 1, http://ec.europa.eu/energy/gas_electricity/smartgrids/doc/2009_03_12_mandate_m441_en.pdf.

[12] Directive 2006/32/EC of the European Parliament and of the Council of the European Union of 5 April 2006 on energy end-use efficiency and energy services and repealing Council Directive 93/76/EEC, OJ 27.04.2006, L114/64. The latest date for implementation was 17 May 2008.

basis of the initial proposals for the Dutch smart meters we discuss below. Although the Dutch proposals assumed that smart meters were mandatory to install, no such explicit obligation can be derived from Directive 2006/32/EC. The Directive also does not prescribe how specific the smart metering should be.

In 2009, the Electricity Directive 2009/72/EC and the Natural Gas Directive 2009/73/EC were adopted. These Directives prescribe smart meters in similar wordings as Directive 2006/32/EC: "*In order to promote energy efficiency, Member States (…) shall strongly recommend that electricity undertakings optimise the use of electricity, for example by (…) introducing intelligent metering systems or smart grids, where appropriate*".[13] Both Directives are supplemented with an Annex regarding measures on consumer protection. These Annexes include a requirement that at least 80% of consumers shall be equipped with smart meters by the year 2020, if an economic assessment by 3 September 2012 is positive.[14] This assessment should determine "*all the long-term costs and benefits to the market and the individual consumer or which form of intelligent metering is economically reasonable and cost-effective*". A time-path of 10 years is foreseen for the implementation of intelligent metering systems. In the European Commission Digital Agenda for Europe the goal is set for the member states to agree on common additional functionalities for smart meters by the end of 2011.[15]

In 2011, a new directive on energy efficiency was proposed that will repeal Directive 2006/32/EC.[16] The explanatory memorandum concludes that smart meters have economic benefits: "*Other options with a considerable positive impact compared to their costs are those that (…) provide improved and more frequent information to households and companies on their actual energy consumption through billing and smart meters (…). The [Impact Assessment] shows that all these measures are valuable in reducing the information gap that is one of the barriers to efficiency and could yield major energy savings*". Voluntary measures are considered insufficient to tap all the available potential for savings, hence the need for a revised directive.

While the legal framework is still taking shape, smart meters have been developed and rolled out in several countries. The SmartRegions project published a European Smart Metering Landscape Report in February 2011. This report concludes that, due to a regulatory push by the EU's Third Energy Market Package, a majority of European countries have or are about to implement some form of legal framework for the installation of smart meters.[17] Some countries are labelled 'dynamic movers' because they already have decided about a mandatory rollout, or major pilot projects

[13] Art. 3(11) Directive 2009/72/EC; similarly, art. 3(8) Directive 2009/73/EC.

[14] Directive 2009/72/EC, Annex I, art. 2.

[15] COM (2010) 245 final/2, 26.8.2010.

[16] Proposal for a Directive on energy efficiency and repealing Directives 2004/8/EC and 2006/32/EC, COM(2011)370, 22.06.2011, http://ec.europa.eu/energy/efficiency/eed/eed_en.htm.

For an elaborate description see: *Steering through the maze #5. Your eceee guide to following the approval process of the proposed Energy Efficiency Directive*, http://www.eceee.org/EED.

[17] Stephan Renner et al., *European Smart Metering Landscape Report SmartRegions Deliverable 2.1.,* 2009, p. 1, http://www.smartregions.net.

are paving the way for such a decision.[18] Besides the Netherlands, countries such as Denmark, Finland, France, Ireland, Italy, Malta, Norway, Spain, Sweden and the UK are 'dynamic movers.' A second category, comprised of Germany, the Czech Republic, Estonia, Slovenia and Romania, is named 'market drivers' where rollout is not based on legal requirements but on internal synergetic effects or because of customer demands. Some countries are labelled ambiguous movers, as the debate is still ongoing without any clear decisions, such as Portugal, Belgium and Austria. The remaining member states are categorised as 'waverers' and 'laggards', as the debate on smart metering has not at all, or just yet, started.[19]

12.2.2 European Legal Framework on Privacy and Data Protection

Privacy can be seen as an umbrella concept, covering different dimensions of private life. The territorial dimension relates e.g. to respect for the home, bodily integrity concerns the right to privacy in relation to the body, the right to choose which relationships to enter into is known as relational privacy, and informational privacy concerns the protection of personal data. Because of the importance of data protection in current society, the concepts of privacy and data protection are often used as synonyms, in a sense that people speak of privacy when they mean informational privacy or the protection of personal data. However, it is important to remember that privacy is a broader notion, encompassing more dimensions than just protection of personal data. This is captured in article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR), which covers the right to respect for private and family life, home and correspondence. This includes many aspects of data protection.[20] The Charter of Fundamental Rights of the European Union includes separate articles stipulating the right to private and family life, home and communications (art. 7) and the right to protection of personal data (art. 8).[21]

Since smart meters potentially involve both personal data and private life, home and communications, they require a comprehensive privacy impact assessment. In the European context, the major legal instruments for such an assessment are the Data Protection Directive for informational privacy and article 8 ECHR for privacy in general.

---

[18] Idem.

[19] See for a graph of these categories: http://www.smartregions.net/default.asp?SivuID=26927.

[20] Cf. Paul De Hert and Serge Gutwirth, "Data Protection in the Case Law of Strasbourg and Luxembourg: Constitutionalization in Action", In *Reinventing Data Protection?*, ed. Serge Gutwirth et al., (Berlin: Springer, 2009), p. 3–45.

[21] The Lisbon Treaty makes the EU Charter of Fundamental Rights a binding and legally enforceable part of EU law, see http://europa.eu/lisbon_treaty/glance/index_en.htm.

For a downloadable copy of the Charter see: http://eur-lex.europa.eu/LexUriServ/site/en/oj/2007/c_303/c_30320071214en00010016.pdf.

12.2.2.1 Directive 95/46/EC[22]

With regard to the informational privacy dimension, several legislative initiatives have been taken in Europe. Within the information society free flow of information is very important. Differences in national data protection legislation can hamper the internal market and from a human rights perspective a high level of protection is desired to protect individuals' personal data. These two pillars form the basis of Directive 95/46/EC, which stipulates the main rights and obligations to be respected when processing personal data.

The Directive constitutes a layered system consisting of three levels. The first level is the general level that applies to every processing of personal data. The second level, which needs to be applied on top of the first level, applies when sensitive data are being processed. The third level is applicable when personal data are being transferred to third countries. Hence, if sensitive data are being transferred to third countries, all three levels apply.

First, it must be determined whether or not Directive 95/46/EC is applicable, on the basis of the first four articles of the Directive. The main questions to be answered are: are *personal* data being processed, i.e., 'data relating to an identified or identifiable natural person' (data subject), and if so, whether an exception applies that makes the processing fall outside of the scope of the Directive.[23] If the Directive applies, personal data "*may only be processed fairly and lawfully*" (art. 6(a)). What this entails, can be derived from the other provisions in the Directive. The main aspects concern the requirement of a specified purpose for processing personal data, the requirement to have a legitimate basis for processing personal data, and the requirement only to process data in a way that is compatible with the specified purpose. Regarding the quality of the data it is determined that data must be relevant, accurate, not excessive and up to date. Besides, sufficient security measures need to be taken in order to protect data from being leaked, corrupted, or destroyed. Furthermore, the data controller (i.e., the one who determines the purposes and means of the processing of personal data) has the obligation to inform data subjects

[22] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281, 23.11.1995, p. 31–50. The Directive has its roots in Convention 108 and the OECD privacy principles, http://conventions.coe.int/Treaty/EN/Treaties/Html/108.htm, http://www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,00.html.

[23] See art. 3: '(1) This Directive shall apply to the processing of personal data wholly or partly by automatic means, and to the processing otherwise than by automatic means of personal data which form part of a filing system or are intended to form part of a filing system. (2) This Directive shall not apply to the processing of personal data: in the course of an activity which falls outside the scope of Community law, such as those provided for by Titles V and VI of the Treaty on European Union and in any case to processing operations concerning public security, defence, State security (including the economic well-being of the State when the processing operation relates to State security matters) and the activities of the State in areas of criminal law; [or] by a natural person in the course of a purely personal or household activity.'

(and in some cases the Data Protection Authority,[24] art. 18) regarding data processing. Data subjects have the right to access, rectification, erasure, blocking, and the right to object to data processing. The Directive obliges Member States to put in place effective sanctioning mechanisms.

The second level lays down an extra strict regime for the processing of sensitive data, being data 'revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life' (art. 8). Even though on the surface this prohibition might not seem relevant in view of smart meter data, examples can be given where these data do provide an insight into, e.g., religious beliefs, as energy consumption can reveal patterns of, for example, observing Ramadan or getting ready for morning prayers.

The third level of the Directive concerns the transfer of data to third countries, which is only allowed if the receiving country ensures an adequate level of protection (art. 25–26). This is not immediately relevant for smart metering, except if suppliers outsource their data processing to non-EU countries or to the cloud.

Besides the general provisions of Directive 95/46/EC, there are also some sector-specific rules and regulations, such as Directive 2002/58/EC and Directive 2006/24/EC which apply to electronic communications.[25] These Directives could play a role when electronic communications services are used for data processing in smart metering systems.[26] These services might, depending on the technologies used and the specifications of the system, process not only personal data but also location data. An analysis of these Directives in relation to smart metering is beyond the scope of this paper; we recommend further research into the applicability of Directive 2002/58/EC to smart metering and, if it applies, into the consequences of this legal regime for smart metering systems.

Finally, the general and specific legislation is supplemented by sector-specific soft law, such as codes of conduct. Such supplementary instruments need to be taken into account as it can influence upon whether and how data may be processed.

---

[24] The Directive obliges all Member States to establish a supervisory authority, also known as Data Protection Authority.

[25] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), OJ L 201, 31.7.2002, p. 37–47. Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, OJ L 105, 13.4.2006, p. 54–63.

[26] The definition of an electronic communications service is: 'a service normally provided for remuneration which consists wholly or mainly in the conveyance of signals on electronic communications networks, including telecommunications services and transmission services in networks used for broadcasting, but exclude services providing, or exercising editorial control over, content transmitted using electronic communications networks and services; it does not include information society services, as defined in Article 1 of Directive 98/34/EC, which do not consist wholly or mainly in the conveyance of signals on electronic communications networks' (art. 2(c) Directive 2002/21/EC, OJ L108/33, 24.4.2002).

In the case of smart metering, the underlying contracts between consumers and energy suppliers can contain specific provisions regarding whether and how personal data may be processed.

12.2.2.2 Proposed Regulation for Data Protection

On Data Protection Day 2012, a Proposal was presented for a new EU General Data Protection Regulation.[27] There is no scope in this paper for elaborate reflection on the consequences of this proposal, since it is a draft that will be much debated and possibly amended in the coming years, and the large-scale roll-out of smart metering may take place prior to the entry into force of the proposed changes. Moreover, a substantial part of the Regulation clarifies and harmonizes existing concepts, rights and obligations of the current EU legal framework on data protection. Some important new rights are proposed, such as the right to be forgotten and a right to data portability (art. 17 and 18). For smart metering, two new obligations can be considered most relevant. Article 23 of the proposed Regulation introduces the principle of privacy by design and default. Establishing an obligation for the controller to implement appropriate technical and organisational measures and procedures to meet the requirements of the Regulation and to ensure the protection of data subject rights. These mechanisms must ensure by default that only those personal data are processed which are necessary for each specific purpose of the processing and are especially not collected or retained beyond the minimum necessary for those purposes.

In article 33 the popular notion of Data protection impact assessment (also known as PIA, Privacy Impact Assessment) is introduced. If data processing operations present specific risks, controllers must carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. Several situations are mentioned, including "*a systematic and extensive evaluation of personal aspects relating to a natural person or for analysing or predicting in particular the natural person's economic situation, location, health, personal preferences, reliability or behaviour, which is based on automated processing and on which measures are based that produce legal effects concerning the individual or significantly affect the individual*" (art. 33, section 2, under a).

As will be discussed in Sect. 12.4.1, smart metering data can offer sharp insights into our daily lives. Therefore, under the proposed new EU legal framework, the introduction of smart metering systems will require not only privacy by design and by default, but also a Data protection impact assessment prior to the implementation

[27] Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), Brussels, 25.1.2012 COM (2012) 11 final 2012/0011 (COD). Available from: http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf.

of such a system.[28] This is a development to which the developers of smart metering systems should adapt in any case, as will become clear from the Dutch smart metering case in Sect. 12.3.

12.2.2.3 The Triple Test of Art. 8 ECHR

As explained above, processing personal data according to data protection legislation is no guarantee that privacy will not be infringed. In smart metering, the consequences of data processing go beyond the informational privacy dimension, as insight can be given into patterns of living, at what times of the day and days of the week someone is at home or away, how many people make up the household, and incidental and structural changes in these patterns over time. If smart metering comes with supply regulation functions, for example if energy supply can be reduced or completely cut off through the meter, there can even be a restriction in a primary necessity of life, which can constitute an invasion of privacy as well.

For European countries, article 8 ECHR is the most important codification of the fundamental human right to privacy. A significant body of case-law helps to apply art. 8 ECHR to new cases and developments. Therefore, a privacy test can best be conducted along the lines of Article 8 ECHR. This article states:

1. Everyone has the right to respect for his private and family life, his home and his correspondence.
2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

The text of article 8 displays a triple test regarding whether or not the right to privacy is invaded. For smart metering, this test translates into the following four questions:

1. Does the smart meter interfere with privacy? If so, the next questions must be answered.
2. Is the infringement in accordance with the law?
3. Does the infringement serve any of the interests mentioned in art. 8(2)?
4. Is the infringement necessary in a democratic society?

Although the first three questions can usually be answered rather easily in respect of smart metering,[29] the fourth question requires to check whether the infringement of

[28] Conducting a PIA is also a core recommendation in the NIST *Guidelines for Smart Grid Cyber Security: Vol. 2, Privacy and the Smart Grid*, NISTIR 7628, August 2010. Available from: http://csrc.nist.gov/publications/nistir/ir7628/nistir-7628_vol2.pdf.

[29] See also Paul de Hert and Dariusz Kloza, "The challenges to privacy and data protection posed by smart grids", In *Europäische Projektkultur als Beitrag zur Rationalisierung des Rechts*, ed. E. Schweighofer and F. Kummer (Wien, 2011), p. 194.

privacy caused by the smart metering system is necessary in view of a pressing social need, relevant to meet its purpose, does not go beyond what is necessary to meet its purpose, and whether there are no less invasive alternatives to meet its purpose (subsidiarity) and its benefits are in a reasonable proportion to the costs (proportionality). This is not easy to assess in general as this closely depends on the specific implementation of smart metering, e.g., whether or not a smart meter is mandatory, the purposes for which it is implemented, and the functionalities that will be given to the smart metering system.

12.3 The Dutch Case[30]

12.3.1 The 2008 Smart Metering Bills

The introduction of smart meters was envisioned by the Netherlands in 2006, with a view to ensuring the smooth operation of the retail energy market.[31] The introduction was also a consequence of the compulsory implementation of the Directive on energy efficiency.[32] This Directive, whose primary aim is to bring about energy savings, prescribes that end users should have energy meters that provide information about actual use. End users must also regularly receive information about this use.

To ensure timely implementation of the Directive, it was decided that this would take place in two stages. The transposition of the Directive would take place in the Implementation of the EC Directives on Energy Efficiency Bill. This bill was submitted to the Second Chamber in January 2008.[33] When another bill, amending the Electricity Act 1998 and Gas Act to improve the operation of the electricity and gas markets (31374 Bill),[34] would enter into force, the provisions with respect to electricity and gas from the Implementation Bill would lapse.

Together, these two smart metering bills provided for the mandatory introduction of so-called smart meters in every Dutch household. Not accepting the installation of a smart meter was made punishable as an economic offence, sanctioned with a fine of up to 17,000 euro or imprisonment for a maximum of 6 months. The smart meter would record and forward to the network operators (also called grid managers) data about consumers' energy consumption at detailed interval periods, namely hourly measurements for gas and quarter-hourly measurements for electricity. These

[30] For the complete parliamentary history of the Dutch implementation of Directive 2006/32/EG see: http://www.eerstekamer.nl/wetsvoorstel/31374_verbetering_werking#p4, http://www.eerstekamer.nl/wetsvoorstel/31320_wet_implementatie_eg, http://www.eerstekamer.nl/wetsvoorstel/32373_novelle_wet_implementatie_eg (only available in Dutch).

[31] Parliamentary Documents Second Chamber 2005/06, 28 982, No. 51.

[32] Directive 2006/32/EC. See supra s. 2.1. The Directive had to be implemented by 17 May 2008.

[33] Parliamentary Documents Second Chamber 2007/08, 31 320, No. 2.

[34] Parliamentary Documents Second Chamber 2007/08, 31 374, No. 2.

data would be forwarded to the energy suppliers, who would then use these data to provide consumers with detailed information about their energy consumption, so that the consumers could adapt their energy-consuming behaviour accordingly.

Besides the measuring and communication functionalities, the initial Dutch proposals also included signaling, switching and regulatory functions. The signaling function enables the network operator to detect energy quality remotely. The switching function enables network operators to remotely switch energy capacity off and on, in order to deal with fraudulent or non-paying customers, or in case of disasters. Finally, the regulatory function entails the possibility to add options to the meter so that it can carry out additional supportive functions.[35]

Since some privacy concerns were raised after the 31374 Bill had been submitted to parliament, the Dutch Data Protection Authority (DDPA)[36] was asked to advise on the Bill. The DDPA deemed the initial proposal for the Dutch smart metering act to violate the Dutch Data Protection Act (Wet bescherming persoonsgegevens). Their main concerns related to a lack of consent or any other legitimate processing ground and obscurities regarding which parties have access to what measuring data.[37] The Minister of Economic Affairs amended the proposal by providing that the network operator could only transfer the hourly or quarter-hourly readings of energy consumption to energy suppliers if consumers have given explicit consent for this; daily readings would, however, still be mandatorily forwarded to energy suppliers. The Minister also emphasised that all conditions of the Dutch DPA would apply, including the requirements of purpose specification and use limitation, data subjects' right of access, data removal after use, and suitable security measures. After the amendment, the Dutch Data Protection Authority deemed the legislation compliant with the Dutch Data Protection Act. Reassured by the amendments, in July 2008, the Second Chamber passed both smart metering bills without any further substantial privacy debate.[38]

12.3.2 Privacy Assessment Report

As data protection is only one dimension of the broader right to privacy, the Dutch Consumer Union was not convinced that all privacy concerns had been addressed. After the bills had been passed by the Second Chamber, the Consumer Union commissioned a study to test whether the proposed smart metering legislation was in

[35] Parliamentary Documents Second Chamber 2007/08, 31 374, No. 3, p. 14.

[36] In Dutch: College Bescherming Persoonsgegevens (CBP), www.cbpweb.nl. English website: http://www.dutchdpa.nl/Pages/home.aspx.

[37] Wetgevingsadvies, 17 juni 2008, z2008-00769, available from: www.cbpweb.nl.

[38] Parliamentary Proceedings Second Chamber 3 July 2008, p. 105–7642.

conformity with article 8 ECHR. This study was conducted by us and published in October 2008.[39]

The report observed that the generation of quarter-hourly/hourly and daily readings from which information can be derived about lifestyles and the presence or absence and numbers of persons, along with the compulsory use of smart meters that generate detailed readings and pass them on to grid managers, as well as the imposition of a severe security obligation on grid managers, are aspects of the bill that infringe privacy. Smart meters put pressure not only on informational privacy, but also on the right to inviolability of the home and the right to respect for family life. For these reasons, the report performed a strict privacy-compliance test as laid down in art. 8 ECHR.

The report concluded that the following characteristics of the proposed Dutch smart metering system were not (proven to be) necessary in a democratic society: the generation and passing on of quarter-hourly/hourly readings to grid managers; the daily readings to grid managers and suppliers; and the compulsory roll-out of smart meters to all households. Therefore, the report concluded that the introduction of the smart meter on these points would violate article 8 of the ECHR.

Moreover, the report found that the government had provided too little evidence to assess the necessity of building in a switching function that would enable capacity to be switched on and off remotely, and a signalling function for combating fraud. To meet the test of article 8, more empirical evidence should be provided about the prevalence of energy fraud, to substantiate the necessity of building in these functionalities for all consumers. After all, these functionalities introduce new opportunities of abuse, e.g., by malevolent hackers, and thus constitute a security and privacy risk.

The main reason for these conclusions was that the bills, particularly the points concerning detailed metering data and compulsory use, provide insufficient substantiation as to why these steps would be necessary in a democratic society. It is not clear whether it would actually foster energy savings – the primary purpose of the Directive – if consumers have to consult their energy consumption on a website provided by their supplier or a third party; it could be equally or more effective if consumers consult their real-time energy use on a display in the house itself, without meter readings having to leave the privacy of the home. In as far as the smart meter was intended to increase efficiency, this aim could be achieved by the proposal, but this is not a pressing social need. There are alternatives that entail less invasive infringements of privacy, again meters with in-home displays can be mentioned, as well as the use of statistical and anonymised data, which might also effectively serve the intended aims. These alternatives had not been sufficiently researched, meaning that the compulsory introduction of smart meters did not meet the requirements of subsidiarity and proportionality. With the bills, insufficient consideration

[39] Colette Cuijpers and Bert-Jaap Koops, *Het wetsvoorstel 'slimme meters': een privacytoets op basis van art. 8 EVRM* [The 'smart meters' bill: a privacy test based on article 8 ECHR], Study commissioned by the Dutch Consumers' Association, October 2008. The Dutch version is available from: http://www.consumentenbond.nl/morello-bestanden/209547/onderzoek_UvT_slimme_energi1.pdf. An English version can be obtained from the authors.

had been given to the fact that the smart meter is a measure that constitutes a significant breach of the right to inviolability of the home and the right to respect for family life. To justify such a breach, much more substantiation with convincing arguments and empirical data was required. In the absence thereof, so the report concluded, the proposal in its current form would therefore have to be rejected.

The report recommended to study suitable alternatives that would infringe privacy to a lesser extent while still contributing to achieve the intended objectives. With respect to installing the switching and signalling functions, additional empirical research could be performed to determine whether these need to be introduced on a large scale.

12.3.3 Rejection by the First Chamber

The Dutch First Chamber discussed the privacy concerns that had been raised by the report and by criticisms that had been voiced in the media. Senators voiced criticism that an ex ante assessment of art. 8 ECHR had not been conducted, observing that the Dutch DPA had only looked at compliance with the Dutch Data Protection Act, and they questioned the Dutch additions to the requirements of the Directive, in the detailed readings of the meter that had to be provided to the network operator and (in daily measurements) to the energy supplier, which consumers could not opt out of. The Senate was not convinced by the Minister's argumentation that art. 8 ECHR was not violated by the proposal. Most importantly, the Senate was particularly alarmed by the mandatory character of the roll-out, and by the far-reaching sanction of 6 months' imprisonment for consumers refusing to have a smart meter installed. Therefore, on April 7 2009, the First Chamber decided not to accept the proposed legislation unless it were changed in several respects.[40] Constitutionally, the First Chamber can only accept or reject bills, but not amend them. In cases like this, the First Chamber can – under threat of rejecting a bill altogether – induce a minister to promise to introduce a new bill, called a 'novella' (*novelle*), in the Second Chamber that amends the bill at issue. This construction allows the First Chamber to accept the original bill as it will be amended by the *novelle*.

12.3.4 The 2010 Novelles

The *novelles* (one for each bill) were introduced in the spring of 2010.[41] Four changes were implemented by the *novelles* that are relevant in view of privacy. Two have only minor privacy implications. First, a so-called supply model

[40] See Parliamentary Proceedings First Chamber, 24 March 2009, 26–1316/1331, 26–1343/1359, and 26–1381/1389; 7 April 2009, 28–1413/1427.

[41] Parliamentary Documents Second Chamber 2009/10, 32 373, No. 2, and 32 374, No. 2.

(*Leveranciersmodel*) was introduced, i.e., a system where end users no longer receive separate bills from the grid manager and the energy supplier. With the introduction of the supply model they only receive one combined bill from their energy supplier. This change is relevant in view of privacy as this change creates coherence between the administrative processes of grid operators, energy suppliers, and measuring companies regarding the management of end-user data.

A second minor improvement for privacy is the duty for the energy sector to address in their annual reports how they have dealt with the requirements regarding data processing. Although it does not enhance the level of privacy as such, it does improve transparency and awareness.

A major change enhancing the privacy-friendliness of the Dutch smart metering landscape concerns cancelling the obligatory roll-out of smart meters. The *novelles* explicitly grant end users the right to refuse a smart meter, without risking a fine or imprisonment, as the sanction is lifted. Besides declining a smart meter, consumers are offered a possibility to request the operator to 'administratively shut down' the smart meter. This means that a grid operator will stop reading measuring data of an end user. A grid operator is legally obliged to honour this request.

A second considerable improvement for privacy is a clarification and codification of the terms and conditions under which personal data can be processed by the parties involved in the process of energy supply. The collection of end-user metering data by the grid manager and energy suppliers is now explicitly tied to their legally prescribed tasks, such as billing by suppliers and network management by the grid operator. This is a refinement of the rules regarding the processing of measuring data. Previously, only the conditions under which grid operators were allowed to transfer measuring data of end users to suppliers were laid down. The conditions now in place regarding the collection and use of such data by grid operators provide more checks and balances to protect the privacy of consumers.

Dutch Parliament was satisfied with the privacy improvement of making the smart meters voluntary. The Second Chamber passed the *novelles* in November 2010 and the First Chamber accepted the original smart metering bills, including the amendments made by the *novelles*, in February 2011.[42]

12.3.5 Privacy Re-assessment

The new Dutch smart metering legislation has clearly responded to the privacy concerns that were one of the main reasons for the First Chamber to reject the earlier proposals. The current Dutch legislation can be described as a four-choice-model, as end users are in a position to choose between four options to measure their energy consumption.

[42] Parliamentary Proceedings Second Chamber, 9 November 2010, 19–18; First Chamber, 22 February 2011, 19-2-2.

1. No smart meter, hold on to the traditional ('stupid') meter.
2. A smart meter that can be administratively shut down.
3. A smart meter with a standard measurement regime.
4. A smart meter for which explicit consent is given to read out more data than is allowed under the standard measurement regime.[43]

Not only the possibility to decline a smart meter is a step towards a more privacy-friendly system, also the fact that grid operators are not allowed to collect a continuous stream of measuring data certainly is an improvement for privacy.[44] In the standard measurement regime, only the following data are allowed to be processed: once a year for the annual invoice; at an intermediate time in case of relocation of the end user or if the end user switches from one energy supplier to another; bi-monthly for an insight into the actual energy consumption; and, finally, all data processing that is relevant for technical management and necessary in view of the legal obligations for grid operators. Data processing thus is also allowed to check for the proper and secure functioning of meters. Moreover, legislation stipulates that grid operators may only transfer data to energy suppliers that are necessary in view of the suppliers' tasks.[45] Hence, daily measurements no longer form part of the standard measurement regime. More frequent and detailed readings of metering data are only permitted if end users have given their unambiguous consent. This consent can be withdrawn at any time without negative consequences for the end user.[46]

Although the scope of this paper does not allow us to assess in-depth the amended legislation's compliance with art. 8 ECHR, for the moment we incline to thinking that the Dutch law is now more in line with privacy requirements. Important factors are that very detailed regular readings are no longer part of the standard measurement regime and that consumers have the right to refuse a smart meter. This significantly reduces the infringement of individuals' privacy.

There is one caveat, however, in that Directives 2009/72/EC and 2009/73/EC foresee a mandatory 80% coverage if a cost/benefit analysis is positive for a member state. According to the Minister, five factors will be taken into account: how often consumers switch to other (presumably more cost-efficient) energy suppliers, the roll-out percentage, roll-out efficiency, the costs of distance-readable meters, and energy savings by consumers. All factors will be closely monitored during the initial small-scale and subsequent large-scale roll-out.[47] The caveat is that the

[43] Parliamentary Documents Second Chamber 2009–2010, 32 374, No. 3, p. 8–9.

[44] Colette Cuijpers, "Slim kiezen bij slimme meters", *Privacy & Informatie,* June 2011, p. 134.

[45] These tasks are listed in article 16 of the *Elektriciteitswet* (Electricity Act) and article 10 of the *Gaswet* (Gas Act).

[46] Parliamentary Documents Second Chamber 2009–2010, 32 374, No. 3, p. 8–9.

[47] Parliamentary Documents First Chamber 2010–2011, 32 373, C. Note that some criticism has been voiced against the assumptions of a KEMA report that serves as a basis for the cost/benefit assessment, debating to what extent benefits of energy savings or supplier switching can be uniquely attributed to smart metering. See Sjak Lomme (2010), 'Commentaar', http://www.energeia.nl/column.php?ID=108.

cost/benefit assessment could turn out positive while less than 80% of consumers accept smart meters. In that case, pressure could be put on unwilling consumers to accept a smart meter after all, jeopardising the voluntary nature of the roll-out. One could question whether a mandatory 80% roll-out target (conditional upon a cost/benefit analysis) is necessary in a democratic society, if a member state bases its art. 8 ECHR compliance on voluntary smart metering. However that may be, the abolition of very detailed readings – which is the main privacy-sensitive issue in smart metering – in the standard measurement regime, with consumers having to give unambiguous consent if quarter-hourly or hourly readings are to be transferred to operators or suppliers, seem to take the largest privacy sting out of the Dutch law.

12.4 Lessons for Assessing the Privacy Aspects of Smart Metering

From the Dutch smart metering case, two factors can be highlighted as having been predominant in the rejection of the smart metering bills by the First Chamber: (1) the very detailed readings of smart meters and the transfer of these readings from consumer to grid operator and (of less but still) detailed readings from operator to energy supplier; (2) the compulsory nature of the roll-out, sanctioned by a hefty fine or even imprisonment. Compounding these factors, two other aspects can be highlighted as underlying the problematic introduction of smart metering legislation: (3) a lack of substantiation why the privacy infringement and the compulsory roll-out were necessary; (4) the combination of different functionalities in one smart meter, creating a complex hybrid involving new risks and also confusing the argumentation for the necessity of such a smart metering system. In this section, we will discuss these factors in some more detail.

12.4.1 The Level of Details of Meter Readings

Smart metering data can offer sharp insights into our daily lives. The intensity of this vision 'through the walls of our home' becomes clear from several recent studies. Molina-Markham et al. indicate that it is possible to extract complex usage patterns from smart meter data: knowledge of an appliance's power signature enables identifying individual appliance usage within the aggregate data of a smart meter. Future data mining will likely enable even more refined identification of appliances, such as particular brands or models.[48] Quinn points out that the privacy issue is all the

[48] Andrés Molina-Markham et al., "Private Memoirs of a Smart Meter", *BuildSys* November 2, Zurich, Switzerland 2010: 1, http://www.cs.umass.edu/~kevinfu/papers/molina-markham-buildsys10.pdf., p. 1.

more important as smart meters enable real-time monitoring of energy consumption.[49] Elaborating on this research, Greveler et al. show that smart meter data, when measured in intervals of 4 h, exactly reveal when a person is at home, when he is sleeping and when he is preparing his meals. When using shorter intervals, of minutes or seconds, electric devices can be identified on the basis of use profiles, such as a fridge, coffee machine, washing machine, toaster, microwave, and TV.[50] These data can reveal if someone eats a cold or a hot breakfast, when laundry is done, or whether the kids are alone at home. It is even possible to determine which channel a TV is tuned to, through an analysis of the broadcast programs, particularly if the TV is tuned to a longer program such as a movie. The interfering noise in the meter data of other energy-consuming devices can most likely be filtered out in case movies are watched of 90 min or longer.[51]

This demonstrates that the more detailed smart meter readings are, the more privacy-sensitive the data become. Real-time readings in intervals of minutes can reveal many details of home life and paint a disturbingly clear picture of people's behaviour and preferences. Quarter-hourly or hourly measurements also reveal a rather privacy-sensitive picture, showing behaviour patterns and perhaps some insight in the type of household appliances used. While daily readings are less privacy-sensitive, they are still relevant from a privacy perspective, as they reveal patterns of being at home or away from home, and the number of people at home on a specific day. Here, privacy risks go hand-in-hand with security risks, threatening the inviolability of the home, as would-be burglars could determine on the basis of smart meter data when residents are away from home, and even whether or not they have an electronic security system.[52] More in general, security risks of smart metering systems emerge from automated two-way communication relationships with heterogeneous partners, requiring strong authentication and authorisation mechanisms to secure the transfer of smart meter data.[53]

The lesson here is that smart meters in today's homes not only measure the amount of energy consumption, but also have great potential to reveal what people do when, within the sanctity of their home. The more detailed the readings, the more privacy-sensitive the data become. This is a major factor to take into account when

[49] Quinn, Elias Leake, Smart Metering and Privacy: Existing Laws and Competing Policies (May 9, 2009). Available at SSRN: http://ssrn.com/abstract=1462285 or http://dx.doi.org/10.2139/ssrn.1462285. p. 11.

[50] U. Greveler, B. Justus, and D. Löhr, "Hintergrund und experimentelle Ergebnisse zum Thema "Smart Meter und Datenschutz"", *Arbeitspapier1 – Technischer Report, Status: ENTWURF, Version 0.6.,* 2011, p. 3.
http://www.its.fh-muenster.de/greveler/pubs/smartmeter_sep11_v06.pdf.

[51] Idem.

[52] Quinn 2009, p. 18.

[53] M. Jawurek and M. Johns, "Security Challenges of a Changing Energy Landscape", In *ISSE 2010 Securing Electronic Business Processes: Highlights of the Information Security Solutions Europe 2010 Convention*, ed. N. Pohlmann, H. Reimer and W. Schneider, (Wiesbaden: Springer Fachmedien 2011), p. 255.

deciding which measurements have to be transferred from smart meters to network operators and energy suppliers. Privacy-sensitive data – such as quarter-hourly or hourly readings but also daily readings – should probably be processed only within the house itself (e.g., in an in-home display that enables consumers to monitor their energy consumption in real time). If detailed measurements are necessary to transfer outside of the home, a very high level of information security must be provided, and compelling reasons must be provided to do so in light of art. 8 ECHR's requirement of 'necessity in a democratic society'.

12.4.2 Mandatory or Voluntary Roll-Out

The largest stumbling block in the Dutch case was the mandatory nature of the roll-out. It was foreseen that every household would receive a smart meter over the course of a few years, and consumers could not refuse. The smart meter bills included a provision that refusing a smart meter would count as an economic offence, which could be sanctioned with up to six months' detention. Although the Minister said in the First Chamber that she would deal with this 'in a practical way', she did not exclude the possibility that network operators would denounce a consumer's refusal with the police and that the Public Prosecutor would then decide how to deal with this economic offence.[54] The combination of mandatory roll-out and the threat of a very serious – indeed, disproportionate – sanction for people who did not want a privacy-infringing smart meter was too much for the bill to survive.

The proposed new Directive on energy efficiency[55] does not seem to require a mandatory roll-out of smart meters. Article 8(1) rather suggests voluntary acceptance of smart meters by end users: "Member States shall ensure that final customers (…) *are provided with* individual meters that accurately measure and allow to make available their actual energy consumption and provide information on actual time of use" (emphasis added). It is questionable that should be interpreted as an obligation on end-users to accept the smart individual meter; the wording suggests they should be provided with the opportunity. Article 8(1) moreover clarifies that certain functionalities are only triggered on request of the final customer: "In the case of electricity and *on request* of the final customer, meter operators shall ensure that the meter can account for electricity produced on the final customer's premises and exported to the grid. Member States shall ensure that *if final customers request it*, metering data on their real-time production or consumption is made available to a third party acting on behalf of the final customer" (emphasis added).

High-frequency interval periods for measurements such as those proposed in the initial Dutch bills are not required on the basis of Annex VI of the proposed Directive. For billing purposes, monthly measurements are foreseen for Electricity

[54] Parliamentary Proceedings 24 March 2009, 26–1385/1386.

[55] COM(2011)370, http://ec.europa.eu/energy/efficiency/eed/eed_en.htm.

and bi-monthly measurements for Gas. For private data exported through the interface to the end user – to better control their energy consumption – the end user must be offered the possibility to consult her historic consumption levels in the last 7 days, day by day. This requires daily measurements. However, the Annex does not require such data to be exported outside of the house: it only requires secured transport of these data from the meter to the end user. For meters placed within a house, an in-home display would therefore suffice to show these daily measurements. Moreover, additional information allowing for more detailed self-checks by customers, such as graphic evolutions of consumption and benchmarking information, should be provided to customers according to Annex VI, but these do not require more detailed than daily readings and these should be accessible to customers "either directly through the interface or via the internet". Hence, the smart meter that seems mandated by the proposed Directive is therefore restricted to one that is capable of at least daily measurements and that has an interface showing readings to the customer. Additional functionality or more detailed readings are not required for a roll-out of smart meters.

This suggests that if countries want to introduce 'smarter' meters than those required by the Directive – particularly if they entail more detailed readings or involve high-frequency transfer of readings to network operators or suppliers – this requires consent of the end users. Knyrim and Trieb, however, have argued that user consent is not necessarily the only possible legal basis for installing smart meters.[56]

> The legitimacy of [smart meter data] transfers has to be based, for example, on a broad interpretation of Articles 7(b) and 7(f) of the Data Protection Directive[57]. Nevertheless, taking into account that (according to almost all academic studies carried out so far) the rollout of new metering technology is economically feasible only if the vast majority of households is furnished with a smart meter, the establishment of a valid legal obligation, either at the European or national level, might serve as the clearest, safest, and most sustainable way of securing successful implementation.[58]

Basically, these authors argue that there is a pressing social need for rolling-out smart meters to a large majority of households, and hence that national legislation mandating end users to accept smart meters would therefore pass the test of art. 8 ECHR. We are not immediately convinced by this argument, first because it requires careful analysis of the studies into the economic aspects of smart metering (something that is lacking in Knyrim and Trieb's article itself), and second because economic arguments are not necessarily strong enough to outweigh privacy interests. Whether legislation mandating smart meters is art. 8 ECHR-compliant will depend on how privacy-infringing they are and on how convincingly a legislator demonstrates that, in the context of the particular country, the economic arguments favouring a comprehensive roll-out of mandatory meters are indeed sufficiently pressing.

---

[56] Knyrim and Trieb, p. 122.

[57] Art. 7(b) refers to execution of a contract and 7(f) to legitimate interests of the data processor that outweigh the privacy interest of data subjects [authors' footnote].

[58] Knyrim and Trieb, p. 128.

For the time being, it seems that European law in itself does not require mandatory smart meters, except for a minimum functionality of daily readings and direct accessibility of these readings to end users, which can be fulfilled through in-home displays. This lays a significant burden of proof on countries that want to roll-out 'smarter' meters than the European minimum on a mandatory basis, to show a 'pressing social need'[59] for this. The experience of the Dutch case suggests it might be a safer strategy to start with a voluntary roll-out and then to closely monitor how the factors evolve that are relevant for assessing the societal costs and benefits of smart meters.

12.4.3 Two Underlying Problems

Although the Dutch case ostensibly revolved around the level of detail of measurements and the mandatory character of the meter, two more general problems can be identified that lay beneath the initial legislative failure.

The first problem is a significant underestimation of the importance of privacy. The drafters of the initial smart metering bills and the Second Chamber focused almost exclusively on the economic and environmental aspects of smart grids and smart meters. No privacy impact assessment had been made. Only when the Dutch Consumer Association pointed out possible privacy concerns to the Minister, did she request the Data Protection Authority to advise on the Bills. When some adjustments had been made following the DPA's advice, the Second Chamber was easily satisfied with the privacy compliance of the smart metering legislation. Throughout this entire process, art. 8 ECHR was overlooked. Only when the privacy assessment report commissioned by the Consumer Association was drafted, did parliamentarians become aware that privacy is more than just compliance with the national Data Protection Act. The fact that smart meters have the capacity to reveal quite privacy-sensitive information, thus affecting not only informational privacy but also privacy of the home and of family life, seems to have been disregarded until the First Chamber, armoured with the privacy assessment report, started questioning the Minister about this. A tell-tale sign of privacy misapprehensions was a complete confusion in the First Chamber discussion whether the Dutch DPA had advised on the basis of compliance with the Dutch Data Protection Act or whether it had checked compliance with art. 8 ECHR. While the Minister initially stated the latter had been the case, subsequently it became clear that it had been the former.[60]

Perhaps because the privacy implications of smart meters had been underestimated, the argumentation for the very detailed readings and the mandatory roll-out had been superficial. An important element of the privacy impact assessment report

[59] ECtHR 24 November 1986, *Gillow* v *The United Kingdom*, App.no. 9063/80, §55.

[60] See Parliamentary Proceedings First Chamber, 24 March 2009, 26–1329, 26-1349f; 7 April 2009, 28–1416.

was that the need for such mandatory 'smartness' had not been substantiated; many claims suffered from a lack of empirical evidence, such as the claim that consumers would become more energy-saving if they received information about their energy consumption from an energy supplier on a website.

The lesson to draw here is not only that privacy implications, of course, should never be underestimated, but also that an ex ante assessment of privacy implications can help to prevent legislative proposals from stumbling over privacy concerns further down the line. Countries considering smart metering legislation should conduct a privacy impact assessment, carefully analysing the privacy implications, and substantiating where appropriate, based on empirical evidence, how and why privacy infringements are deemed necessary in a democratic society. An important element of such a privacy impact assessment is looking at alternatives that are less privacy-invasive but that still serve the intended purposes of smart metering.

The second problem underlying the Dutch case is function creep – the expanding of functionality beyond the original purpose. While the European legislation required smart meters to provide feedback to end users, thus helping them to become more energy-saving, the Dutch bills added several functionalities to the proposed smart meter. Apart from providing information to consumers for energy-saving purposes, smart meters also had to provide distance-readable measurements to monitor network functioning and to combat fraud. Moreover, the meter also had to be controllable at a distance to regulate energy delivery, both for fraud-combating and disaster-management purposes.[61] The combination of all these functionalities led to a smart meter with a potential of very high frequency of two-way traffic between the meter and the grid. The transfer of very detailed measurements to the network operator, and daily measurements to energy suppliers, fitted well in the picture of such a hybrid smart meter, leading to a neglect of privacy-friendly alternatives, such as in-home displays or aggregation of individual meter data in the grid, that could likely equally well have served the purposes of energy-saving or network management. Also, the legitimate need for combating fraud, which can be served well by smart meters, does not necessarily imply that comprehensive, wide-scale processing of detailed meter readings is necessary to identify occasional illegal activity.[62]

The lesson here is that smart meters have a wide range of functionalities,[63] which harbours a risk that too many functions are combined in a smart meter in a way that makes privacy implications less visible or less weighty in the overall assessment of

[61] In Italy, the introduction of smart metering by ENEL was strongly driven by the desire to combat fraud. See in this respect: Rob van Gerwen, Saskia Jaarsma and Rob Wilhite, *Smart Metering,* KEMA, The Netherlands, July 2006. Available from: http://www.idc-online.com/technical_references/pdfs/electrical_engineering/Smart_Metering.pdf.

[62] Cf. Article 29 Working Party, "Opinion 12/2011 on smart metering", WP 183, April 4, 2011, p. 21.

[63] For an overview see: Smart Meters Co-ordination Group (SMCG), *Standardization mandate to CEN, CENELEC and ETSI in the field of measuring instruments for the develop-ment of an open architecture for utility meters involving communication protocols enabling Interoperability M/441*, FINAL REPORT 2009, http://www.piio.pl/dok/SMCG_Sec0013_DC.pdf.

the need for a smart meter.[64] This can backfire if the privacy assessment of a resulting hybrid smart meter concludes that the smart meter as a whole, with all its functionalities, is economically necessary, while disregarding whether privacy infringements are really necessary in light of each separate purpose. In other words, countries proposing complex smart meters with many functionalities may tend to overlook that simple purposes, such as inducing consumers to become more energy-saving or peak-load reduction in network management, can also be achieved by privacy-friendly alternatives.

12.5 Conclusion

The future of energy supply lies in smart grids, which enable not only energy supply to consumers but also energy supply from consumers. These two-way energy networks require smart energy metering systems. The vision of truly smart grids will require one or more decades yet to be fully realised, but since a roll-out of smart meters is a lengthy process, countries are already starting to implement smart metering legislation, following the European legal framework on energy efficiency. Rolling out smart meters, however, requires smart legislation. The Dutch case, where the Senate blocked two smart metering bills in 2009, demonstrates that introducing smart meters can be significantly delayed if the underlying legislation if flawed.

More in particular, the Dutch case shows that privacy is not to be underestimated. The failure of doing an ex ante privacy impact assessment backfired, as the proposed laws required mandatory installation in every household of smart meters that would send quarter-hourly/hourly measurements to network operators and daily measurements to energy suppliers. This level of detail creates privacy-sensitive data, and the necessity of smart meters infringing people's privacy in this way had not been substantiated by the government.

Several lessons can be learned from the Dutch case for countries considering smart metering legislation. In terms of substance, the level of detail of smart meter readings and the mandatory or voluntary character of smart meters are crucial issues to take into account. In terms of procedure, a privacy impact assessment is vital to identify at an early stage the potential effects on individuals' privacy and to choose the least privacy-infringing modalities of smart metering. Pitfalls of function creep should be avoided by resisting the temptation of making a meter 'too smart' all at once, which could easily lead, as the Dutch case demonstrates, to choosing privacy-invasive instead of privacy-friendly settings; such settings are unnecessary to achieve the primary purpose of the current European energy-efficiency regulation, namely

[64] The addition of extra functionalities over and above the requirements of the European Directives was also an issue for the First Chamber in questioning the acceptability of the smart metering bills. See, e.g. Parliamentary Proceedings First Chamber, 24 March 2009, 26–1325.

to provide consumers with sufficient feedback on their energy consumption to induce energy-saving behaviour.

The procedural lessons also highlight the need for privacy by design. This principle concerns the need to integrate, at practical level, data protection and privacy from the very inception of new information and communication technologies.[65] The purpose, design, functionalities and implementation of the smart metering system determines to a large extent whether or not it will comply with privacy and data protection legislation. Therefore, from the beginning, privacy and data protection law must be taken into account as an important requirement for the design of smart metering systems.[66] It is a promising development that the proposed Regulation on data protection explicitly establishes obligations for privacy by design and default, and an ex ante obligation for data protection impact assessments in cases where data processing has specific risks.[67]

The substantive lessons can also be formulated in the form of a key trade-off for legislators: the 'smartness' of the meter versus a comprehensive, mandatory roll-out. The smarter a meter is, i.e., the more detailed its readings are – up to quarter-hourly or even less – and the more functionalities it has, the more likely is it to be privacy-invasive. Current research already shows how revealing smart meter data can be of people's daily life in their homes, and findings such as the capacity to derive which TV channel one is watching from real-time energy readings[68] suggest that the privacy-sensitivity of energy consumption data will only increase in the future. This implies that if countries opt for smart meters with detailed readings that leave the privacy of the home, this can hardly be considered necessary in a democratic society, and hence, such smart meters can only be rolled out on a voluntary basis, as now will happen in the Netherlands. And conversely, if countries choose a relatively 'dumb' meter that conforms to the minimum requirements of European legislation (capable of at least daily measurements and with an interface showing readings to the customer), they can likely make the roll-out of such meters mandatory for consumers, in terms of compliance with art. 8 ECHR.

We would like to end with two concerns that remain even if legislators adopt smart legislation about smart meters. One is the role of consent. If countries opt for a voluntary roll-out of smart meters, are consumers sufficiently informed about what a smart meter entails? In the Dutch case, they can choose not only between keeping their 'dumb' meter and accepting a smart meter, but also, if they accept a smart meter, they can opt for administratively shutting off the detailed readings by

[65] Opinion of the European Data Protection Supervisor on Promoting Trust in the Information Society by Fostering Data Protection and Privacy, Brussels 2010, p. 2, available from: http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2010/10-03-19_Trust_Information_Society_EN.pdf.

[66] See also Knyrim and Trieb, 2011.

[67] Art. 23 and 33 of the Proposed General Data Protection Regulation, COM(2012) 11 final 2012/0011 (COD).

[68] Greveler, Justus, and Löhr, p. 1 and 3.

the network operator or, at the other end of the privacy spectrum, give consent to forwarding detailed readings to energy suppliers or third parties. Whether consumers can make informed decisions about this depends greatly on the information provided to them by the network operator that asks them to have a smart meter installed, and on the way this information is provided. Should operators present the meter without informing consumers that they have a right to refuse, and should they suggest that providing detailed readings to third parties is a normal default setting ('just tick the box here'), then consent would lose its meaning. Moreover, average consumers will not be aware of the privacy impact of smart meter measurements; few will realise – if they are not informed explicitly of this – that daily readings offer insight into when they are away from home, and hardly anyone will be aware of the technical possibilities of deriving life patterns and appliance use from more detailed readings.[69] In short, an important element of a privacy-compliant roll-out of smart meters will be to make sure that consumers are adequately informed of the implications of smart meters.

Our second concern is a more general one. The house is rapidly losing its character as privacy's fortress, with directional microphones recording in-house conversations, cameras seeing through walls, thermal imagers detecting heat emissions, household appliances incorporated in the Internet of Things, the home computer permanently connected to the Internet, and private information such as personal texts, photos, books and music no longer stored in desks or on shelves but instead in the cloud.[70] Smart meters are yet another addition to this increasing transparency of the home. This requires careful consideration of the cumulative effect of the various developments that allow insight into how people live, in the one place where people most of all must feel free to do what they like. If our home will no longer be our castle, the house may be energy-efficient but it will be a cold place to live.

References

Article 29 Working Party, Opinion 12/2011 on smart metering, WP 183, 4 Apr 2011.

Cuijpers, Colette. 2011. Slim kiezen bij slimme meters. *Privacy and Informatie* 14–3: 131–141.

Cuijpers, Colette, and Pekárek Martin. 2011. The regulation of location-based services: Challenges to the European Union data protection regime. *Journal of Location Based Services* 5: 223–241. doi:10.1080/17489725.2011.637081. Accessed 17 Aug 2012.

De Hert, Paul, and Dariusz Kloza. 2011. The challenges to privacy and data protection posed by smart grids. In *Europäische Projektkultur als Beitrag zur Rationalisierung des Rechts*, ed. E. Schweighofer and F. Kummer. Tagungsband des 14. Internationalen Rechtsinformatik Symposions IRIS 2011, Wien, 191–196.

[69] Greveler, Justus, and Löhr, p. 4. http://www.its.fh-muenster.de/greveler/pubs/smartmeter_sep11_v06.pdf.

[70] B.J. Koops and M.M. Prinsen, "Houses of Glass, Transparent Bodies: How New Technologies Affect Inviolability of the Home and Bodily Integrity in the Dutch Constitution", *Information & Communications Technology Law*, 16 (3) 2007, p. 177–190.

De Hert, Paul, and Serge Gutwirth. 2009. Data protection in the case law of Strasbourg and Luxembourg: Constitutionalization in action. In *Reinventing data protection?* ed. Serge Gutwirth et al., 3–45. Berlin: Springer.

ESMA. Annual report on the progress in smart metering 2009. http://www.esma-home.eu/UserFiles/file/ESMA_WP5D18_Annual_Progress_Report_2009%281%29.pdf. Accessed 17 Aug 2012.

Greveler, U., Justus, B. and D. Löhr. 2011. Hintergrund und experimentelle Ergebnisse zum Thema "Smart Meter und Datenschutz", Arbeitspapier1 – Technischer Report, Status: ENTWURF, Version 0.6. http://www.its.fh-muenster.de/greveler/pubs/smartmeter_sep11_v06.pdf. Accessed 17 Aug 2012.

Jawurek, M., and M. Johns. 2011. Security challenges of a changing energy landscape. In *ISSE 2010 securing electronic business processes: Highlights of the information security solutions Europe 2010 convention*, ed. N. Pohlmann, H. Reimer, and W. Schneider, 249–259. Wiesbaden: Springer Fachmedien.

Knyrim, Rainer, and Gerald Trieb. 2011. Smart metering under EU data protection law. *International Data Privacy Law* 1–2: 121–128. doi:10.1093/idpl/ipr004. Accessed 17 Aug 2012.

Koops, B.J., and M.M. Prinsen. 2007. Houses of glass, transparent bodies: How new technologies affect inviolability of the home and bodily integrity in the Dutch constitution. *Information and Communications Technology Law* 16–3: 177–190.

Molina-Markham, Andrés et al. 2010. Private memoirs of a smart meter. BuildSys. Zurich. http://www.cs.umass.edu/~kevinfu/papers/molina-markham-buildsys10.pdf. Accessed 17 Aug 2012.

NIST Smart Grid Interoperability Panel – Cyber Security Working Group. Aug 2010. *Guidelines for smart grid cyber security: Vol. 2, privacy and the smart grid*. NISTIR 7628. Available from: http://csrc.nist.gov/publications/nistir/ir7628/nistir-7628_vol2.pdf. Accessed at August 17 2012.

Quinn, Elias Leake, Smart Metering and Privacy: Existing Laws and Competing Policies (May 9, 2009). Available at SSRN: http://ssrn.com/abstract=1462285 or http://dx.doi.org/10.2139/ssrn.1462285. Accessed 17 Aug 2012.

Renner, Stephan et al. 2009. European smart metering landscape report smartRegions deliverable 2.1. http://www.smartregions.net/default.asp?SivuID=26927.

Smart Meters Co-ordination Group (SMCG) Standardization mandate to CEN, CENELEC and ETSI in the field of measuring instruments for the development of an open architecture for utility meters involving communication protocols enabling Interoperability M/441, FINAL REPORT, Version 0.7 – 2009-12-10. http://www.piio.pl/dok/SMCG_Sec0013_DC.pdf. Accessed 17 Aug 2012.

Task Force Smart Grids, Expert Group 1 (EG1). Dec 2010. Functionalities of smart grids and smart meters. Final Deliverable. http://ec.europa.eu/energy/gas_electricity/smartgrids/doc/expert_group1.pdf. Accessed 17 Aug 2012.

Chapter 13
User Choice, Privacy Sensitivity, and Acceptance of Personal Information Collection

Joshua B. Hurwitz

13.1 Introduction

The issue of data privacy has revolved around the disparate goals of data collectors and data subjects. Data collectors (application and service providers, marketing and advertising companies, etc.) want to collect as much data as possible to maximize the value of advertising and marketing and to guide product and service development to meet the needs of end users. On the other hand, data subjects such as Internet and device users want valuable applications and services at minimal cost.

One of the costs for users is the risk to their privacy (Awad and Krishnan 2006). Privacy risk is considered one of the top concerns of Internet users (Antón et al. 2010). There is evidence that many users avoid using web sites or provide false personal information to sites because of concerns about privacy (Hurwitz 2011).

A further issue is the disparity between the expectations of users and assumptions of data collectors. Web sites, service providers and other entities that acquire users' personal information may assume that this data is public, whereas users may consider it to be private (Adams 2000). This disparity in expectations can result reputational and legal harm for data collectors, as happened when Facebook announced plans to share its users' addresses and phone numbers with developers (Claburn 2011).

A variety of factors appear to influence users' privacy concerns. Research suggests that such concerns are affected by users' perceptions of

1. The sensitivity of collected information (Zhang et al. 2010) and
2. Its relevance to applications and services that collect it (Graeff and Harmon 2002; Lwin et al. 2007)

J.B. Hurwitz (✉)
Motorola Mobility, Applied Research Center, Libertyville, IL, USA
e-mail: jbenhurwitz@gmail.com

S. Gutwirth et al. (eds.), *European Data Protection: Coming of Age*,
DOI 10.1007/978-94-007-5170-5_13,

Such concerns may be ameliorated by enhancing user knowledge of and control over the data collection process (Spiekermann 2007; Stewart and Segars 2002). However, even with greater control, some users may be too privacy sensitive or untrusting to accept applications and services that collect such information (Kumaraguru and Cranor 2005).

The current study was an effort to demonstrate these influences in a mobile application that collects personal information. Specifically, the privacy manager incorporated into this application enables some user control over data collection, but provides incentives for users to permit data collection. One goal was to demonstrate the impact of having such control on user judgments of the privacy-relevant features of the service. Another was to demonstrate how data sensitivity and relevance and user privacy sensitivity and trust can affect acceptance of the service.

What follows is a brief review of research in this area. This review highlights the role that the aforementioned factors play in user perceptions, and is followed by a description of the application used in this study and the hypotheses for the study.

13.1.1 Research Review

13.1.1.1 Properties of Collected Information

Individuals' privacy concerns with respect to a given service are partly influenced by the type of information collected by that service. One of the important attributes of information that affect such concerns is its sensitivity. For example, users are apparently more accepting of collection of information about commercial transactions (Zhang et al. 2008) than about the collection of behavioral information, such as video, in personal spaces (Zhang et al. 2008; Adams and Sasse 1999; Barkuus and Dey 2003).

Data sensitivity affects user intentions to reveal the information. Individuals' concerns over revealing sensitive information increase when this information is collected by organizations they do not trust (Rohm and Milne 2004). Furthermore, information sensitivity apparently influences the effectiveness of incentives to collect that information, since providing a larger incentive reduces privacy concerns only when the information is less sensitive (Yang et al. 2009).

The evidence from prior research also suggests that sensitivity interacts with the relevance of the data to affect user privacy concerns. Relevance (also called "congruence") refers to whether the collected information provides important functionality in the context in which it is collected. For example, a retailer's customers might consider it relevant that the retailer collect information about their purchases in order to provide better discounts. However, those customers would probably perceive information extracted from their text messages as less relevant for this purpose. Users' privacy concerns are apparently greater when they perceive that the collected data is not relevant to the context in which it is collected (Graeff and Harmon 2002), particularly when the information is sensitive (Lwin et al. 2007).

13.1.1.2 User Control

One method for reducing the perceived risk inherent in some activity is to give users more insight into that activity and the perception that they can control it (Slovic 1987). Many web sites, application developers and service providers have been giving users tools to better understand and control their privacy. For example, Facebook has enhanced its tools to control sharing of personal information, and Google provides a dashboard that gives users complete control over storage of their search history (Claburn 2009).

There is a long history of research on how user control over their personal information affects perceived privacy (Spiekermann 2007; Stewart and Segars 2002). Stewart and Segars (2002), in their analysis of an instrument measuring Concern for Information Privacy (CFIP), found the theme of control underlying CFIP. Spiekermann (2007) further elaborated on this concept, highlighting two types of control: control over the collection of personal information and control over the use of that information.

Providing control apparently has positive effects on user privacy perceptions, and improves their awareness of the privacy-relevant aspects of applications and services. For example, Günther and Spiekermann (2005) found that being given more control enhances user trust in services that collect personal information. Furthermore, Consolvo et al. (2010) found evidence that it increases user awareness of potential privacy risks, and Alpert et al. (2003) found that having control increases user awareness of how their interaction with a system has been influenced by the information collected by that system.

While providing greater control may increase users' confidence that their privacy is being protected, Awad and Krishnan (2006) point out that it could also reduce the flow of information to data collectors. This could occur if users frequently reject data collection when given the option to do so. Furthermore, such rejection could occur more often for information that is more sensitive.

13.1.1.3 Trust

Even when users are given some control over their privacy, they cannot control all aspects of information collection, storage and usage. Thus, as Wang and Emurian (2005) point out, vulnerability is an essential component of trust, so that individuals necessarily take a risk when they engage in electronic activities that reveal personal information. To reduce privacy concerns, they must have a certain degree of trust in the motivations and abilities of data collectors, as well as in the adequacy of the data collection infrastructure (clients, transmitters, servers, etc.), to protect their privacy.

As Fan and Chen (2005) point out, trust has been defined in terms of the expectations that individuals have about other entities involved in an interaction. In e-commerce, one factor that can affect trust is the way a data collector, such as a web site or service provider, portrays itself (Turner et al. 2001), including its use of privacy certifications (Xu et al. 2005). Evidence also suggests that trust in a provider can

also be influenced by the duration of exposure to that provider (Büttner and Göritz 2008). It can also be affected by so-called "word-of-mouth" (Kuan and Bock 2007), including information about the provider from trusted sources.

However, aside from these external influences on trust, there is also evidence of a baseline propensity or disposition to trust (Fan and Chen 2005; Lee and Turban 2001; McKnight et al. 2004; Ranaweera et al. 2008). Such a tendency may develop from lifelong socialization (Fan and Chen 2005), and studies have found associations of a tendency to trust with personality characteristics such as innovativeness (Chen 2011) and risk-taking (Colquitt et al. 2007). Furthermore, individuals with a higher propensity to trust also display greater online purchase intentions (Ranaweera et al. 2008; Chen 2011).

13.1.1.4 Privacy Sensitivity

While being more trusting may counteract qualms users may have about disclosing personal information, there is some evidence that privacy sensitivity also feeds into avoidance of applications and services that collect such information. One of the earliest proponents of an index of individual differences in privacy sensitivity was Dr. Alan Westin (Kumaraguru and Cranor 2005). He performed a number of survey studies on privacy attitudes using items that asked about user concerns over threats to privacy, the types of information sought by companies, governmental threats to privacy, consumers' ability to control their privacy, and privacy protections afforded by data collectors' practices and governmental laws and regulations.

Based on his studies, Westin developed a tripartite categorization of privacy concern: Fundamentalists, Pragmatists and Unconcerned. Privacy Fundamentalists do not trust any organizations to protect their privacy, while Pragmatists balance the costs and benefits of providing their personal information. The Unconcerned trust data collectors and are satisfied with existing organizational and governmental regulations and procedures for protecting privacy (Kumaraguru and Cranor 2005).

While Westin's research emphasized attitudes towards data collectors and privacy regulators, other individual differences measures have focused more on attitudes towards the various elements of data collection and privacy protection. For example, the Concern for Information Privacy (CFIP) Scale (Smith et al. 1996) evaluates concerns over the type of data collected, errors in collection and storage, secondary uses of data (e.g., marketing), and privacy breaches and other unauthorized access to personal information. The Internet Uses Information Privacy Concerns (IUIPC) Scale (Malhotra et al. 2004) evaluates, for example, attitudes toward and control over data collection, and individuals' knowledge of procedures companies use to protect privacy.

Beyond Attitudes

While the Westin, CFIP and IUIPC attitude scales have made important contributions to the understanding of individual differences in privacy sensitivity and concern, they suffer from a number of shortcomings. First, even though these instruments

focus on different aspects of privacy concern and understanding, Buchanan et al. (2007) have found evidence that they are significantly correlated with each other. Second, as Buchanan et al. point out, privacy concerns can also be influenced by the benefits of providing personal information, including receiving increased functionality from applications and services. They also highlight that users' privacy concerns can be moderated by their use of technologies for protecting their privacy.

However, a third and more important shortcoming of privacy attitude scales is the finding that users' behaviors often are at odds with their attitudes (Berendt et al. 2005; Jensen et al. 2005). Even users who profess to be concerned about their privacy frequently use their credit card for online purchases or engage in other activities that put their privacy at risk.

Given this disparity, an alternative approach to evaluating privacy sensitivity might be to collect information about users' choices to engage in activities that reveal personal information. Such choices could be indicators of whether users prioritize privacy over the functionality they obtain from those activities.

For example, Hurwitz (2011) found that users' tendencies to take privacy risks are significantly associated with value judgments for services that collect personal information. Using a survey methodology, Hurwitz asked respondents to rate the value of four TV and two mobile services both with and without the collection of personal information. The impact of such collection on ratings was affected by respondents' self-reported tendencies to risk their personal information by electronically sharing it. When data collection was added to the services, value judgments fell significantly more for respondents who typically engage in less sharing than for those who engage in more sharing.

13.1.2 The Mobile Discount Application

Given the foregoing, an alternative conceptualization of privacy concern may be one in which privacy sensitivity modulates individuals' estimates of the costs versus the benefits of using an application or service that collects personal information (Acquisti 2004). Those who are less privacy sensitive may consider more the benefits of the service, while those who have greater privacy sensitivity may consider more the privacy risks, and incorporate those risks into the costs of using the service.

The current study employed a field study methodology in which subjects were given Motorola Milestone phones that came with a prototype mobile discount service called MobileSaver (Fig. 13.1). This service provides users with savings points that can be used to obtain discounts on grocery products when they go shopping. They accumulate savings points as a function of the amount of time they are registered with the service, and spend those points to get discounts on products listed in the MobileSaver application.

The service also provides privacy notifications and disclosures. These include the types of information collected, why it is needed, and how it is protected. Furthermore, when users register for the service, they are provided with a warning about the data collection and a link to the disclosures.

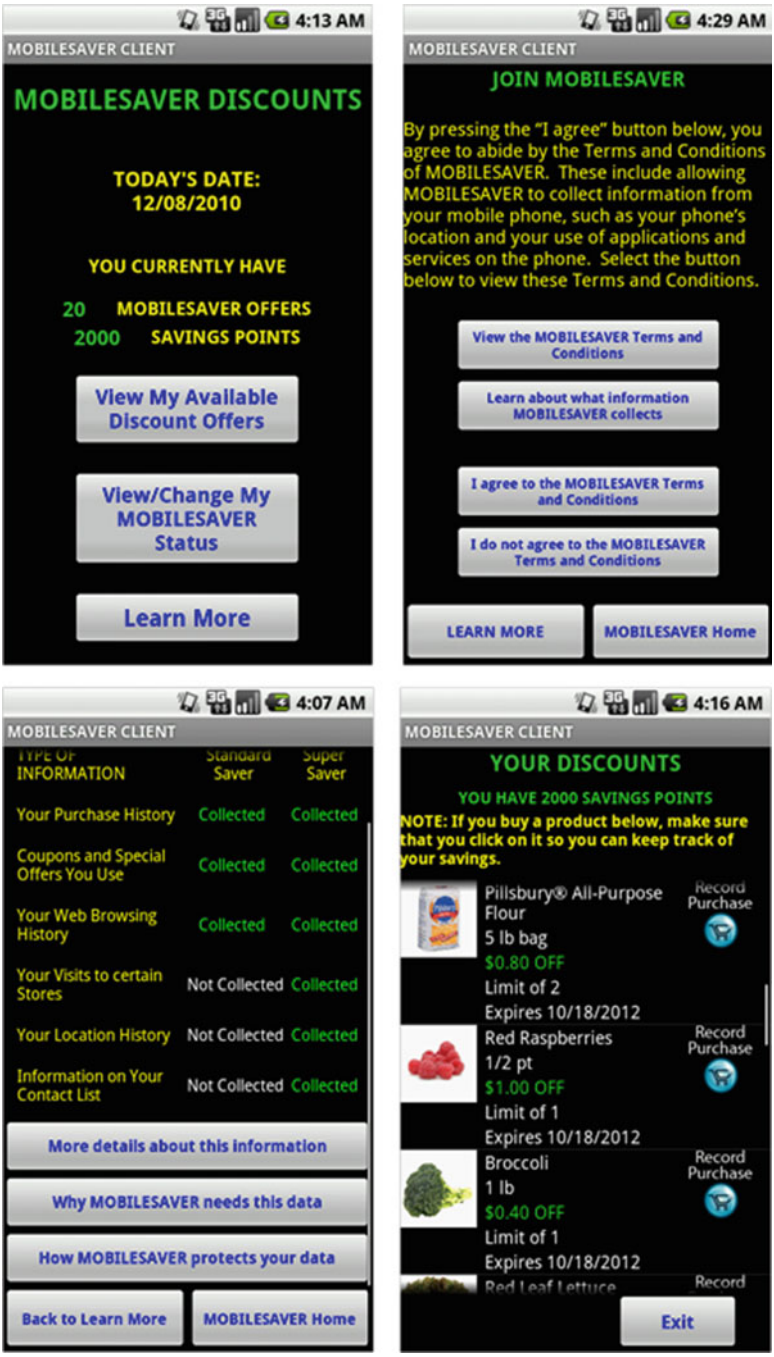


Fig. 13.1 Screen shots of MobileSaver. *Upper left*: The home page; *Upper right*: Opt-in notice; *Lower left*: Disclosure of data collected; *Lower right*: Discount page

13.1.2.1 Savings Programs

When users first launch the MobileSaver application, they are asked to register for the service. As part of this process, the full version of the application asks them to choose between different savings programs. The critical feature of this choice is that if a user opts for a program that offers more savings points, then they must accept more extensive data collection. This involves collection of more types of personal information, including more sensitive information.

As part of the registration process, users are provided with a link to a disclosure that displays the types of information collected for each savings program. They are also presented with a demographics questionnaire which asks about gender, age, income range, household size, and frequency of grocery shopping. While this questionnaire is optional, users are offered bonus savings points for completing it.

13.1.3 Study Hypotheses

The main questions for the current study are the impact of choice, individual differences and types of personal information collected on user perceptions of privacy and acceptance of services that collect their personal information. Given the results of previous studies, being able to choose savings programs in MobileSaver, and thus determine the types of data collected, should enhance user perceptions of their privacy protections. Furthermore, the perceived value of MobileSaver should be influenced by the types of information that this service could potentially collect, as well as users' privacy sensitivity and level of trust. Specifically, perceived value should increase when the service collects information that is less sensitive and is more relevant to providing users with important functionality. Furthermore, when it collects personal information, the perceived value of MobileSaver should be greater for users who are less privacy sensitive and who have greater trust that their privacy will be protected.

13.2 Method and Procedure

There were 24 research subjects in the study, 8 males under 40 years of age, 7 females under 40, 8 females 40 or older, and 1 male 40 or older. All subjects reported that they live in Schaumburg, Illinois and surrounding communities, all had a Smartphone with AT&T mobile service that included a data plan and all reported that they typically shopped for groceries at least four times per month.

All subjects attended a pre-study meeting and a post-study meeting. During the pre-study meeting, they were asked to complete three questionnaires: a demographics questionnaire, a questionnaire on their use of mobile applications, and a questionnaire on their preferred grocery products. Data from the last questionnaire were used to target discount offers in MobileSaver.

Table 13.1 Data collected by each MobileSaver discount program

	Discount program	
Type of information	Standard saver	Super saver
Purchase history	Collected	Collected
Coupons and special offers used	Collected	Collected
Web browsing history	Collected	Collected
Visits to certain stores	Not collected	Collected
Location history	Not collected	Collected
Information on contact list	Not collected	Collected

Also, at this meeting, the subjects were given Motorola Milestone phones with the MobileSaver client application loaded on each phone, and were given instructions for 5-week the field study. They were instructed that they would use Mobile Saver to get discounts on products when they go shopping, and that they should bring in their receipts to the post-study meeting to get reimbursed for the discounts.

For the field study, there were three conditions, with eight subjects assigned to each condition. In the User-Control condition, the MobileSaver user interface gave them the option of choosing 1 of 2 discount programs: Standard Saver or Super Saver. They could save more money in Super Saver than in Standard Saver, up to $20 per week versus $10, but more information was collected by the service in the Super Saver program (Table 13.1).

Aside from this User-Control condition, there were two Non-User-Control conditions: a High-Incentive condition and a Low-Incentive condition. The subjects in the High-Incentive condition were not given a choice of savings program, but the savings and information collected were equivalent to those in the Super Saver program. Those in the Low-Incentive condition were also not given a choice, except the available savings were equivalent to the Standard Saver program.

13.2.1 Post-study Questionnaires

At the end of 5-week field study, the subjects came back for individual post-study meetings at which they completed several questionnaires and were paid for their participation. The questionnaires were a Service Usage questionnaire, a questionnaire on their Choice of MobileSaver Program, two Individual Differences questionnaires, and questionnaires on Information Sensitivity, Information Relevance and Value of MobileSaver.

13.2.1.1 Service Usage

The 4-item "Service Usage" questionnaire asked about subjects about their grocery shopping frequency and frequency of using MobileSaver during the field study. In this questionnaire, 21 subjects ("Participants") indicated that they had registered for

and used MobileSaver, and three subjects ("Non-Participants") indicated that they had not. The Participants were then presented with the questionnaires described below, along with a number of other questionnaires that are not discussed in the current paper.

13.2.1.2 Choice of MobileSaver Program

Participants in the User-Control condition were asked their reasons for their choice of MobileSaver program. In particular, they were asked how much their choice was due to the amount of money they could save versus protection of their privacy.

13.2.1.3 Individual Differences

The two individual-differences measures of interest were the tendency to take privacy risks and the tendency to trust that data privacy will be protected. After Hurwitz (2011), three of the items from the Questionnaire on "Sharing Personal Information" were used to derive a privacy-risk measure. This questionnaire asks users to indicate how often they perform each of eight activities involving taking or avoiding privacy risks. The three items used for the analyses presented here asked subjects how often they did the following:

- "Share your personal pictures or videos with other people using the Internet or using mobile messaging"
- "Use a micro-blogging service, such as Twitter, to share your current activities with other people"
- "Respond to phone marketing surveys"

An index of the subject's privacy-risk tendency was computed using the median of their ratings on these items. Each subject was then placed into a "High Sharing" group if their index was above the median index value for all subjects. Otherwise, they were placed into the "Low Sharing" group.

Trust

Subjects' tendencies to trust that their data privacy will be protected were computed based on their responses to two of the items in the "Trust" Questionnaire. These items, which were taken from a survey on privacy developed by Alan Westin (Kumaraguru and Cranor 2005), asked how much subjects agree that

- "Most businesses handle the personal information they collect about consumers in a proper and confidential way."
- "Existing laws and organizational practices provide a reasonable level of protection for consumer privacy today."

An index of each subject's trust levels was computed based on the average of their responses to these items. They were then placed in one of two groups based on

Table 13.2 Categories of information presented in the information sensitivity, information relevance and MobileSaver value questionnaires

Coupons and special offers you use	Your purchase history
Entries in your calendar	Your social network
Information on your contact list	Your use of mobile applications
Mobile entertainment you download and use	Your visits to certain stores
Your location history	Your web browsing history
Your mobile communications	Your web searching history

this index. They were put into a "High Trust" group if their index value was greater than the median index value for all subjects. Otherwise, they were placed in the "Low Trust" group.

13.2.1.4 Information Sensitivity, Relevance and Value

Subjects were presented with questionnaires asking for their opinion about information that could be collected by MobileSaver. Table 13.2 shows the types of information presented in these questionnaires. Two of these questionnaires, on information sensitivity and relevance, were used to categorize these types of information. The third questionnaire, about MobileSaver value, was used as a dependent measure in the analyses below.

The measure of sensitivity for a given type of information was derived from a questionnaire asking subjects to identify, among the 12 types of information, the 5 that they would consider to be the most sensitive. Information about an activity was considered "sensitive" if the subject was not "comfortable" with MobileSaver collecting that information. The six information types that had the highest average ranking were considered "High Sensitive", and the remaining information types were considered "Low Sensitive".

The measure of relevance was derived from a questionnaire asking subjects to rate how relevant the information categories in Table 13.2 are for providing them with functionality in MobileSaver. This questionnaire, which was completed by 12 of the 21 MobileSaver Participants, instructed them to respond using the following 4-point Likert scale: Totally Irrelevant, Moderately Irrelevant, Moderately Relevant, and Totally Relevant.

For the purposes of the analyses below, an information type was considered relevant based on its average relevance rating. The six information types with the highest average ratings were labeled as having "High Relevance", and the remaining ones were labeled as having "Low Relevance".

The final questionnaire asked MobileSaver Participants to judge whether it would be worth using MobileSaver if it collected each type of information shown in Table 13.2. They were instructed to give their response on the following 4-point Likert scale: Definitely not Worthwhile, Probably not Worthwhile, Probably Worthwhile and Definitely Worthwhile.

13.3 Results

13.3.1 Use of the MobileSaver Service

Most subjects, 21 out of 24, registered for MobileSaver without cancelling the service, and these Participants used the service for an average of 34.7 days (s.d. 1.85 days). All except one of these subjects completed the optional registration questionnaire. Among those who did not use MobileSaver, two never registered and one cancelled the service without using it. After these subjects were excluded, there were eight subjects in the User-Control condition, seven in the Low-Incentive condition, and six in the High-Incentive condition.

Among those subjects who registered for MobileSaver, seven opened the "Terms and Conditions" page, viewing it for an average of 29.0 s. (s.d. 22.0). Five subjects opened the privacy disclosure pages, which provide user-friendly descriptions of what data is collected, why it is collected and how it is protected. The subjects who opened one or more of these pages viewed them on average for 45.8 s. (s.d. 67.9).

The subjects who registered for and used MobileSaver used this service for an average of 38%(s.d. 19 %) of the days during which they were registered. On average, they viewed 3.2 pages (s.d. 2.3) per day in the application, and used it for an average of 2.6 min. (s.d. 0.87) per day. They viewed the list of offers 0.29 times each day (s.d. 0.21), and redeemed an average of 0.20 offers (s.d. 0.25) each day. On average, they redeemed 7%of the 20 offers that were available each week.

13.3.1.1 Demographic Differences in Usage

There were significant gender and age differences in the use of MobileSaver. In general, older females used this service more than younger females, who used it more than males. Compared to males, older females viewed significantly more pages per day in MobileSaver (4.7 vs. 2.0, $t(11)=2.45$, $p<.05$, $r^2=0.35$). Older females tended to view more pages than younger females (4.7 vs. 2.9), and younger females tended to view more pages than males (2.9 vs. 2.0). However, these comparisons were not statistically significant (older vs. younger females: $t(13)=1.80$, $p<.10$, $r^2=0.20$; younger females vs. males: $t(13)=1.87$, $p<.10$, $r^2=0.23$).

Older females also tended to redeem more MobileSaver offers than did males (11.9 vs. 3.2), although this result was marginally significant ($t(13)=2.18$, $p<.06$, $r^2=0.30$). They also redeemed more offers than younger females (11.9 vs. 6.0), who redeemed more than males (6.0 vs. 3.2), but these last comparisons were not significant ($p<0.2$).

13.3.1.2 Choice of Savings Program

When subjects had a choice of savings program, six reported that they initially chose the Standard Saver program, and three reported first choosing the Super Saver

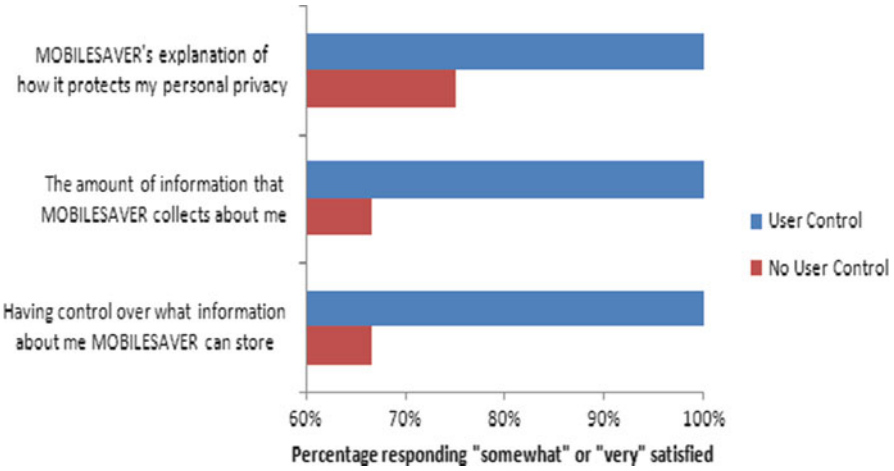


Fig. 13.2 Percentage of subjects in each user-control condition indicating satisfaction with privacy-relevant features of MobileSaver

program. Three of these subjects reported changing their choice. For their final choice—the program that they spent the most time in—five subjects reported that they chose Standard Saver and four reported that they chose Super Saver. However, one subject who reported that their final choice was Super Saver actually had chosen Standard Saver.

Among the reasons for choosing a savings program, two subjects who reported choosing Standard Saver indicated that their choice was based mostly or entirely on the money they could save, even though they could save more with Super Saver. The other three subjects who reported choosing Standard Saver attributed their choice mostly or entirely to privacy considerations. All four subjects who reported choosing Super Saver indicated that they considered mostly or only the savings.

13.3.2 Post-study Questionnaires

13.3.2.1 Impact of Control, Usage, and Incentives

Several trends were observed in the results that suggest a potentially positive effect on users who had been given some control over the data collection process. On average, subjects who were given some control indicated greater satisfaction with "[h]aving control over what information about me MOBILESAVER can store" (Fig. 13.2), although this result was a non-significant trend ($\chi^2(1)=3.33$, $p<0.07$, $\phi=0.41$). The same trends were observed for "[t]he amount of information that MOBILESAVER collects about me" ($\chi^2(1)=3.33$, $p<0.07$, $\phi=0.41$) and "MOBILESAVER's explanation of how it protects my privacy" ($\chi^2(1)=2.35$, $p<0.15$, $\phi=0.34$).

Usage of MobileSaver was also associated with subjects' reported satisfaction with privacy-relevant aspects of MobileSaver. For the purposes of this analysis, the subjects were divided into two groups: "High-Use" subjects who used MobileSaver more than the median percentage of the days (36 %) during which they were registered for the service, and "Low-Use" subjects who used it less than the median percentage of days. All High-Use subjects responded that they were "somewhat" or "very" satisfied with the control they had over information collection, whereas only 60% of Low-Use subjects indicated these levels of satisfaction ($\chi^2(1)=5.44$, $p<0.05$, $\phi=0.51$). The same result was observed for satisfaction with MobileSaver's privacy protections ($\chi^2(1)=5.44$, $p<0.05$, $\phi=0.51$). Finally, while a greater percentage of High-Use than Low-Use subjects (91% vs. 70 %) were satisfied with the amount of personal information collected by MobileSaver, this difference was not statistically significant ($p<0.5$).

In the "No-User-Control" conditions, a greater percentage of subjects in the High-Incentive condition than in the Low-Incentive condition (83% vs. 57 %) were satisfied with the amount of information collected by MobileSaver, but this result was not statistically significant ($p<0.3$). Other than this trend, there were no differences between these groups in their satisfaction with the amount of control over data collection and MobileSaver's privacy protections.

13.3.2.2 Information Sensitivity

Results of rankings of the sensitivity of information and of its relevance for MobileSaver showed that the most sensitive types of data were location and web-searching histories, as well as calendar and contact-list information, mobile communications, and social-networking information. For the purposes of the analyses presented below, these items were considered "High Sensitive". The least sensitive were coupons and special offers used, preferred mobile entertainment, purchase history, store visits, use of mobile applications and web browsing history, so these were classified as "Low Sensitive".

The types of information that were given the highest rankings for relevance were location, web-searching, and purchase histories, as well as coupons and special offers used, preferred mobile entertainment, and visits to certain stores. These were classified as "High Relevance" items. The lowest-ranked items for relevance were calendar and contact-list information, mobile-communications and social-networking information, use of mobile applications and web-browsing history. These were classified as "Low Relevance" items.

13.3.2.3 Impact on Service Value

Subjects' judgments of MobileSaver were apparently influenced by the sensitivity and relevance of the data that could be collected by this service. These judgments were also influenced by their tendencies to take privacy risks, and by their trust in companies and regulations to protect their privacy.

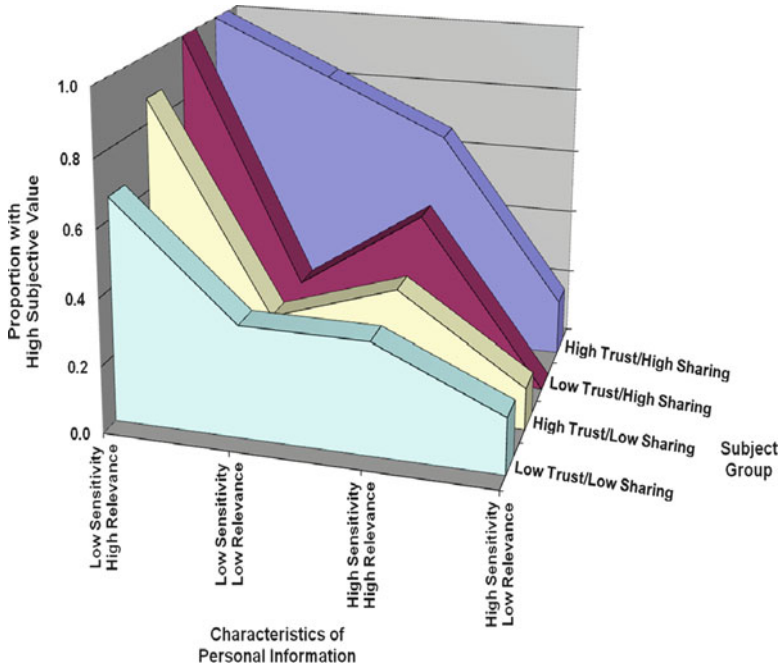


Fig. 13.3 The proportion of subjects who indicated it would "probably" or "definitely" be worthwhile to use MobileSaver even if it collected their personal information, for each subject group and type of personal information

As shown in Fig. 13.3, these factors affected whether subjects considered MobileSaver worthwhile using when it collects their personal data ($F(1, 77) = 14.49$, Adj MSErr = 0.33, $p < .001$, $R^2 = 0.16$). Specifically, ratings of whether MobileSaver was worthwhile using were highest for low-trust/low-sharing subjects and low-sensitive/high-relevant information. These ratings decreased with decreasing subject trust and sharing, increasing data sensitivity and decreasing data relevance ($F(1, 77) = 364.4$, Adj MSErr = 0.33, $p < .001$, $R^2 = 0.83$).

13.4 Discussion

The results of this study support the idea that user acceptance of services that collect personal information is likely to be enhanced if data collectors employ a multifaceted approach to dealing with users' privacy concerns. Such an approach should include the development of tools that give users some control over privacy-relevant decisions, including decisions on data collection, storage and usage. This approach should also include the development of metrics to better understand how users perceive the information being collected; specifically their perceptions of the sensitivity of the data and of its relevance to the services through which it is being collected.

Finally, effective privacy management should involve a better understanding of users' privacy sensitivities and of their trust in data collectors.

One trend in the results was that being given some control produced greater satisfaction with MobileSaver's privacy protections. While this result was a non-significant trend, it is line with other research showing that such control has beneficial effects on user privacy concerns, including increasing trust in data collectors (Günther and Spiekermann 2005). Increased trust can, in turn, enhance users' willingness to make online purchases (Gefen 2000) and disclose personal information online (Paine et al. 2007). Thus, rather than making users more cautious about self-disclosing, giving them greater control over their privacy may actually increase the amount of information they are willing to provide.

However, providing greater control also gives users more insight into the data collection process (Consolvo et al. 2010). Thus, users who are given some control over data collection for a service will likely have greater knowledge of the types of data that service could collect. The results of this study suggest that, when given a choice, users are likely to reject the collection of sensitive data, especially when they perceive that it is not relevant to the functionality provided by a service. Furthermore, the results suggest that this is more likely to occur with users who are more privacy sensitive and less trusting of data collectors.

13.4.1 Assessing Individual Differences

One contribution of this research is that privacy sensitivity was measured based on subjects' reports of their prior behaviors, rather than their attitudes. Furthermore, this metric, when combined with a measure of trust, was strongly related to subjects' value judgments. That is, subjects who reported being more trusting and taking more privacy risks with their personal information also gave higher ratings to the question of whether MobileSaver would be worth using, even if it collects personal information. This was especially true if the collected information was either more relevant and sensitive, or less sensitive and relevant.

The approach taken here overcomes the problems inherent in using attitudinal measures. Not only does it avoid the issue of attitudes being at variance with behaviors, but it is also more concrete and more easily interpretable. For example, consider the following items:

3. Indicate how much you agree or disagree with [the following] opinion: Consumers have lost all control over how personal information about them is circulated and used by companies.
4. Indicate how often you perform [the following] activity: Share your personal pictures or videos with other people using the Internet or using mobile messaging.

Item 1, from the Westin scales, requires survey respondents to subjectively interpret phrases such as "lost all control" and "personal information". However, item 2, which comes from the Sharing scale used in the current study, requires that subjects only recall how frequently they engage in a concrete activity involving well-defined objects (e.g., pictures) and media (e.g. the Internet).

The index of privacy sensitivity used here—the tendency to electronically share personal information—could also be derived from user behavioral data, instead of a survey. This is potentially a convenient and simple measure that could help data collectors better understand the sensitivities of their user population. Also, data collectors can collect this information with minimal risk to the privacy of their users. For example, they would need only record the frequency of sharing, and not what content is shared and with whom.

13.4.2 Limitations

While the results of the current study suggest novel approaches to privacy management, one shortcoming of this study is the small sample size. This limitation is especially an issue for evaluating individual differences, and could account for the fact that group differences in satisfaction with MobileSaver's privacy protections were not statistical significant. A study with a larger sample and longer exposure to an application might confirm the significance of these trends.

A second issue is the limited control users were given in the User-Control version of the service. The choice in MobileSaver was limited to two savings programs, and affected only what data could be collected. A future privacy management system might give more extensive control, including what types of information can be collected, how it can be used, and with whom it can be shared. Enhancing users' privacy management tools in this way may produce larger effects on user satisfaction than those that were observed in this study.

13.4.3 Conclusions

Despite these limitations, the current study did find important results that could guide the development of privacy management systems. If the findings from this study are supported by future research, they suggest that user control may increase user satisfaction with the privacy-relevant features of a service. The implication of this result, along with the results from other prior research, is that user control is likely to increase user trust. This should reduce the perceived risk of using applications and services due to privacy concerns.

However, in order to assure that providing control will be effective, application developers and service providers need to understand the privacy sensitivities and trust levels of their user population, as well as how users perceive the sensitivity of collected data. Such understanding could help avoid the disparity between data collectors' and users' understanding of whether the collected data is public or private. The avoidance of such a disparity could increase user acceptance of data collection. However, such increased acceptance can only occur if users perceive that the collected data is relevant for improving the functionality of the application or service that collects the data.

References

Acquisti, A. 2004. Privacy in electronic commerce and the economics of immediate gratification. In *ACM electronic commerce conference (EC'04)*. New York: ACM.

Adams, A. 2000. Multimedia information changes the whole privacy ballgame. In *Proceedings of the tenth conference on computers, freedom and privacy: Challenging the assumptions*. Toronto: ACM.

Adams, A., and M.A. Sasse. 1999. Privacy issues in ubiquitous multimedia environments: Wake sleeping dogs, or let them lie? In *INTERACT'99*. Edinburgh.

Alpert, S.R., et al. 2003. User attitudes regarding a user-adaptive eCommerce web site. *User Modeling and User-Adapted Interaction* 13(4): 373–396.

Antón, A.I., J.B. Earp, and J.D. Young. 2010. How internet users' privacy concerns have evolved since 2002. *IEEE Security and Privacy* 8(1): 21–27.

Awad, N.F., and M.S. Krishnan. 2006. The personalization privacy paradox: An empirical evaluation of information transparency and the willingness to be profiled online for personalization. *MIS Quarterly* 30(1): 13.

Barkuus, L., and A. Dey. 2003. Location-based services for mobile telephony: A study of users' privacy concerns. In *The 9th IFIP TC13 international conference on human-computer interaction (INTERACT 2003)*. Zurich.

Berendt, B., O. Günther, and S. Spiekermann. 2005. Privacy in e-commerce: Stated preferences vs. actual behavior. *Communications of the ACM* 48(4): 101–106.

Buchanan, T., et al. 2007. Development of measures of online privacy concern and protection for use on the internet. *Journal of the American Society for Information Science and Technology* 58(2): 157–165.

Büttner, O.B., and A.S. Göritz. 2008. Perceived trustworthiness of online shops. *Journal of Consumer Behavior* 7(1): 35–50.

Chen, T. 2011. Personality traits hierarchy of online shoppers. *International Journal of Marketing Studies* 3(4): 23–39.

Claburn, T. 2009. Google dashboard rnhances privacy control. [Cited 2001 Mar 29]; Available from: http://www.informationweek.com/news/internet/google/showArticle.jhtml?articleID=221600693.

Claburn, T. 2011. Facebook faces congressional privacy interrogation. InformationWeek. [Cited 2011 December 1]; Available from: http://www.informationweek.com/news/internet/social_network/229201226.

Colquitt, J.A., B.A. Scott, and J.A. LePine. 2007. Trust, trustworthiness, and trust propensity: A meta-analytic test of their unique relationships with risk taking and job performance. *The Journal of Applied Psychology* 92(4): 909–927.

Consolvo, S., et al. 2010. The Wi-Fi privacy ticker: Improving awareness & control of personal information exposure on Wi-Fi. In *UbiComp '10*. Copenhagen: ACM.

Fan, Y.W, and J.C. Chen. 2005. The moderating effect of disposition to trust in online services. In *10th annual meeting of Asia-Pacific decision sciences institute*. Taipei.

Gefen, D. 2000. E-commerce: The role of familiarity and trust. *Omega: The International Journal of Management Science* 28(6): 727–737.

Graeff, T.R., and S. Harmon. 2002. Collecting and using personal data: Consumers' awareness and concerns. *Journal of Consumer Marketing* 19(4): 302–318.

Günther, O., and S. Spiekermann. 2005. RFID and the perception of control: The consumer's view. *Communications of the ACM* 48(9): 73–76.

Hurwitz, J. 2011. The influence of trust and privacy risk-taking on user acceptance of electronic services that collect personal information. In *2011 meeting of the human factors and ergonomics society*. Las Vegas: The Human Factors and Ergonomics Society.

Jensen, C., C. Potts, and C. Jensen. 2005. Privacy practices of internet users: Self-reports versus observed behavior. *International Journal of Human Computer Studies* 63(1–2): 203–227.

Kuan, H.-H., and G.-W. Bock. 2007. Trust transference in brick and click retailers: An investigation of the before-online-visit phase. *Information Management* 44(2): 175–187.

Kumaraguru, P., and L.F. Cranor. 2005. *Privacy indexes: A survey of Westin's studies*. Pittsburgh: Carnegie Mellon University.

Lee, M.K.O., and E. Turban. 2001. A trust model for consumer internet shopping. *International Journal of Electronic Commerce* 6(1): 75–91.

Lwin, M., J. Wirtz, and J.D. Williams. 2007. Consumer online privacy concerns and responses: A power–responsibility equilibrium perspective. *Journal of the Academy of Marketing Science* 35: 572–585.

Malhotra, N.K., S.S. Kim, and J. Agarwal. 2004. Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model. *Information Systems Research* 15(4): 336–355.

McKnight, D.H., C.J. Kacmar, and V. Choudhury. 2004. Dispositional trust and distrust distinctions in predicting highand low-risk internet expert advice site perceptions. *e-Service Journal* 3(2): 35–58.

Paine, C., et al. 2007. Internet users' perceptions of 'privacy concerns' and 'privacy actions'. *International Journal of Human Computer Studies* 65(6): 526–536.

Ranaweera, C., H. Bansal, and G. McDougall. 2008. Web site satisfaction and purchase intentions: Impact of personality characteristics during initial web site visit. *Managing Service Quality* 18(4): 329–348.

Rohm, A.J., and G.R. Milne. 2004. Just what the doctor ordered: The role of information sensitivity and trust in reducing medical information privacy concern. *Journal of Business Research* 57: 1000–1011.

Slovic, P. 1987. Perception of risk. *Science* 236: 280–285.

Smith, H.J., S.J. Milberg, and S.J. Burke. 1996. Information privacy: Measuring individuals' concerns about organizational practices. *MIS Quarterly* 20(2): 167–196.

Spiekermann, S. 2007. Perceived control: Scales for privacy in ubiquitous computing. In *Digital privacy: Theory, technologies and practices*, ed. A. Acquisti et al. New York: Taylor & Francis.

Stewart, K.A., and A.H. Segars. 2002. An empirical examination of the concern for information privacy instrument. *Information Systems Research* 13(1): 36–49.

Turner, C.W., M. Zavod, and W. Yurcik. 2001. Factors that affect the perception of security and privacy of E-commerce web sites. In *Fourth international conference on electronic commerce research*. Dallas.

Wang, Y.D., and H.H. Emurian. 2005. An overview of online trust: Concepts, elements, and implications. *Computers in Human Behavior* 21: 105–125.

Xu, H., H.-H. Teo, and B.C.Y. Tan. 2005. Predicting the adoption of location-based services: The role of trust and perceived privacy risk. In *Twenty-sixth international conference on information systems*. Las Vegas.

Yang, S., Y. Wang, and Wang K-l. 2009. The influence of information sensitivity compensation on privacy concern and behavioral intention. *SIGMIS Database* 40(1): 38–51.

Zhang, H., et al. 2008. Privacy issues and user attitudes towards targeted advertising; A qualitative focus group study. Motorola.

Zhang, H., et al. 2010. Privacy issues and user attitudes towards targeted advertising: A focus group study. In *Annual meeting of the human factors and ergonomics society*. San Francisco.

Chapter 14
Beyond Gut Level – Some Critical Remarks on the German Privacy Approach to Smart Metering*

Frank Pallas

14.1 Introduction

The introduction of smart metering has strongly concerned privacy advocates over the past few years. All over the world, governments are pushing for a modernization of electricity infrastructures and, in particular, for a development towards "Smart Grids" by means of a strongly escalated pervasion with information and communication technologies (ICT). The motivations behind these developments are manifold, ranging from a more active participation of customers to a better integration of renewables.

Smart Metering, in turn, is one of the integral core technologies of Smart Grids. The data basis provided under the traditional paradigm of mechanical, manually read meters does by far not suffice to achieve the pursued goals. Smart Meters, in contrast, can be read out remotely without significant cost and thus in much higher frequency, thereby establishing the much more detailed and more timely data basis that is indispensable for the development of the more dynamic, adaptive and "intelligent" electricity grids that we will need in the future to achieve the societal goals of climate protection, security of supply, and economic efficiency.

In order to make these developments possible in the first place, the European Union included in the directive on common rules for the internal market in electricity (2009/72/EC) the requirement that all member states shall "ensure the implementation of intelligent metering systems" whereas "at least 80% of consumers shall be

*The author is indebted to Oliver Raabe, Eva Weis and Mieke Lorenz for intensive and fruitful discussions on the subjects examined herein and for helpful comments on earlier drafts of this document.

F. Pallas (✉)
Karlsruhe Institute of Technology, Center for Applied Legal Studies, Karlsruhe, Germany

Computers and Society, Technical University of Berlin, Berlin, Germany
e-mail: frank.pallas@kit.edu

S. Gutwirth et al. (eds.), *European Data Protection: Coming of Age*,
DOI 10.1007/978-94-007-5170-5_14, © Springer Science+Business Media Dordrecht 2013

equipped with intelligent metering systems by 2020."[1] In response to this directive, countries across Europe have started to roll-out smart meters or have at least started to make preparations for such a roll-out, thereby laying the groundwork for the aspired modernization of electricity grids.

On the other hand, the introduction of smart meters raises serious privacy concerns. In particular, this refers to high resolution consumption data (e.g. one value for each 15-min interval) that is explicitly or implicitly associated with individual customers or households. Such data may provide deep insights into individual habits and behavior and therefore affects the customers' data protection rights. This fact has largely been recognized by data protection authorities, consumer associations and activists across Europe and elsewhere,[2] leading to intensive discussions about how privacy should be protected within the Smart Grid.

In the light of these discussions and being well aware of the possibly far-reaching privacy implications of smart metering, the German legislator explicitly addressed privacy aspects in his recent amendment to the national energy law that implements the electricity directive and basically declares the installation of smart meters compulsory.[3] Data protection authorities as well as technical security specialists from the Federal Office for Information Security (Bundesamt für Sicherheit in der Informationstechnik, BSI) were strongly involved in the legislative process from the very beginning, leading to an amendment that contains several privacy-related provisions and serves as an anchor for a whole program of subsequent regulations, protection profiles and technical guidelines that shall ensure a privacy-friendly establishment of smart metering and, in the end, smart grids in Germany.

The German approach to data protection in smart metering and smart grid environments shall therefore be presented and critically discussed herein. In particular, this will be done with regard to the existing regulatory givens of the electricity market. Any sustainable approach for realizing privacy-friendly smart grids must also take into account these givens as defined, for instance, by the European directive 2009/72/EC and its different national implementations. Even if this regulatory framework is of course not carved in stone and may very well be altered in the future, it does at least define the current status quo and must therefore not be ignored when reflecting on possible approaches to a privacy-friendly design of smart grid technologies. To allow for well-founded and practically relevant considerations, the main principles and concepts of the European electricity market and the respective regulations shall therefore be outlined in Sect. 14.2.

---

[1] Directive 2009/72/EC, Appendix I, Number 2. Both requirements can be subject to a national "economic assessment of all the long-term costs and benefits". We will, however, abstract from this restriction herein.

[2] See, for instance, Article 29 Data Protection Working Party, "Opinion 12/2011 on Smart Metering," http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp183_en.pdf, accessed Nov. 28, 2011; Trans Atlantic Consumer Dialogue, "TACD Recommendations for Governments and Utility Service Providers: Smart Meters Need Customer-Centered Standards," http://tacd.org/index.php?option=com_content&task=view&id=175&Itemid=43, accessed Nov. 28, 2011.

[3] There are some restrictions to this obligation, but these can be assumed to become nearly irrelevant in the medium term. See Sect. 14.5.3 below.

In order to establish a sound understanding of the motivation behind the introduction of smart metering and smart grids, we will outline the fundamental challenges having to be dealt with in the future and explain how the introduction of smart metering and smart grids is aspired to counteract them. This is done in Sect. 14.3. In Sect. 14.4, we will then give a general overview of the potential drawbacks of smart metering and smart grids with regard to data protection. Based on these fundamental givens, we will then introduce the established status quo of German energy data communication, delineate the "novel approach" to smart meter communication and privacy that underlies the recently amended energy legislation in some more detail and briefly summarize two other paradigms for energy data communication pursued elsewhere in Europe (Sect. 14.5).

This "novel approach" will then be discussed with regard to the goals that the introduction of smart grids is aimed at as well as in the light of the regulatory givens and the alternative communication paradigms laid out before (Sect. 14.6). Some implications for a potential adoption of the German approach under other national legislations or even on a European level are derived from this discussion in Sect. 14.7. Section 14.8 sums up.

14.2 The European Electricity Market

The regulatory basis for all of our further considerations is given by the European directive 2009/72/EC on the internal market in electricity. In particular, this directive defines the main actors, roles and principles structuring European electricity markets. At the heart of this regulation lies the concept of unbundling, which shall ensure that the ownership and operation of electricity networks is strictly separated from other down- or upstream activities like electricity generation or the supply to final customers. This is done to prevent owners or operators of networks from exploiting their natural monopoly by discriminating against their competitors in up- or downstream markets.

The market structure established to prevent such discrimination rests on four fundamental roles which have to be strictly distinguished from each other. These roles are[4]:

- The *producer*, who operates the facilities that generate electricity (power plants, wind parks, etc.). Generated electricity is then sold on the wholesale market to other parties (especially to suppliers, see below) and fed into the network that the generating facility is connected to.
- The *transmission system operator (TSO)*, who operates the interconnected extra-high-voltage network for long-line transmission within a given geographic area. In most cases, generated electricity is currently fed into the transmission system.

[4] The delineation used herein generalizes from the accurate definitions given in article 2 of the directive to a certain extent for reasons of lucidity. The actual regulations are even more complex than depicted here due to different exceptional rules. To understand the general preconditions for reflecting on the energy market, however, the generalized model used herein should be sufficient.

- The *distribution system operator (DSO)*, who operates a local lower-voltage network for ultimately distributing electricity from a transmission system to final customers.
- The *supplier*, who buys electricity from producers and sells it to customers, using the physical networks operated by the TSO and the DSO for transmission and delivery.

Based on these fundamental market roles, the above-mentioned unbundling is primarily realized through two constraining regulations which can be found in articles 9 and 26 of the directive. Both ensure a non-monopolistic provision of up-or downstream services under conditions of actual competition.

- Article 9 refers to *TSO unbundling* and prescribes that TSOs and parties exercising direct or indirect control over a TSO may at the same time exercise (direct or indirect) control neither over a producer nor over a supplier.
- Article 26, in turn, refers to *DSO unbundling* and basically allows a DSO to be part of a "vertically integrated undertaking" that combines the DSO-role with at least one of the roles of generator/supplier. But even in this case, the DSO that is part of the vertically integrated undertaking shall be independent from the other parts regarding legal form, organization and decision making.

These roles and restrictions form the fundamental regulatory basis for any endeavor to establish smart grids and smart metering in Europe and have to be carefully taken into account when reflecting on data protection aspects within these fields. Any communication architecture that is to be established for reading out and handling individual measurement data must allow these actors to fulfill their legally assigned obligations in full conformance with the mentioned unbundling rules. This fundamental requirement will also persist under the paradigm of smart grids which shall be briefly outlined next.

14.3 Smart Grids at a Glance

The reasons for establishing smart grids are manifold and cannot be laid out exhaustively here.[5] The core requirements for energy data communication can, however, also be illustrated on the basis on just one of the main goals to be served by smart grids: The provision of network stability under conditions of increasingly used renewable sources of generation.

[5] For respective overviews see, for example, European Commission, "European SmartGrids Technology Platform – Vision and Strategy for Europe's Electricity Networks of the Future," (EUR 22040, 2006) http://ec.europa.eu/research/energy/pdf/smartgrids_en.pdf, accessed Nov. 28, 2011; European Commission, "ICT for a Low Carbon Economy – Smart Electricity Distribution Networks," (2009) http://ec.europa.eu/information_society/activities/sustainable_growth/docs/sb_publications/pub_smart_edn_web.pdf, accessed Nov. 28, 2011; International Energy Agency, "Technology Roadmap Smart Grids," (2011), http://www.iea.org/papers/2011/smartgrids_roadmap.pdf, accessed Nov. 28, 2011.

The overarching goal of any electricity infrastructure is to ensure a reliable and cost-efficient supply of customers. From a technical perspective, this requires that generation and consumption of electricity exactly equal each other at any single moment within an interconnected network. Currently, this equalization is primarily realized by adjusting generation to the consumption that is predicted for a certain moment and by employing additional reserve capacities that can quickly respond to discrepancies between predicted and actual demand. Smaller exceptions notwithstanding, the equalization thus mainly takes place at the generation side today.

With increasing proportions of electricity generated from fluctuating, non-controllable sources like wind and solar, this paradigm does not hold anymore. As generation from these sources can not be adjusted to the respective demand without significantly wasting available "green electricity" by switching off facilities and as electricity can not be stored efficiently in substantial amounts, the only way to significantly increase the proportion of renewables and reduce the use of fossil energy sources while at the same time equaling generation and demand is to make adjustments on the demand side.

This, in turn, requires the introduction of some sort of variable price schemes that do, at least to a certain extent, motivate customers to use electricity at times of high generation from renewables and low demand instead of times with low generation from renewables and high demand. To actually implement such variable price schemes, new mechanisms are needed for billing the customers on the basis of non-static prices, which can only be done by smart meters that measure the consumed amount of electricity in comparably high resolution.

Billing the respective customer on the basis of dynamic prices is, though, by far not sufficient. In particular, a changed consumption behavior on the user side must also find its way back into the mechanism that harmonizes generation and demand. Due to the above-mentioned paradigm of unbundling, multiple suppliers use the same transmission and distribution system for delivering the electricity generated by multiple producers to their customers. Maintaining network stability therefore requires all these suppliers and producers to cooperate with each other and ensure that overall generation estimates overall consumption for any single moment.

This is realized in different ways across Europe, but in most cases some sort of balancing mechanism is used that obligates any single supplier to procure electricity that exactly equals the aggregated consumption of his own customers for any single time-slot of 15 or 30 min. The enforcement of this mechanism requires the respective (aggregated) consumption values to be fed into the balancing mechanism. Currently, the necessary values are usually generated by statistical means from long-term consumption values, but with the more dynamic, generation-oriented (e.g. "weather-adaptive") consumption behavior aspired for the future, this practice will not suffice anymore. Instead, real (aggregated) measurement values will have to be fed into the balancing mechanism in one way or another in order to allow suppliers to procure electricity in dependence on actual, intentionally changed consumption behavior.

For this and many further ways of supporting downstream processes throughout the whole energy system in order to afford higher energy efficiency, security of supply, and a significantly increased use of renewable energy sources like wind and solar,

high resolution measurement data collected by means of smart metering is indispensable. On the other hand, high-resolution measurement of electricity consumption also raises serious concerns with regard to data protection.

14.4 Data Protection and Smart Metering

Data protection issues have significantly influenced the discussion about the introduction of smart grids and smart metering from the very beginning on. As it has repeatedly been noted, electricity consumption data can provide meaningful insights about the person(s) that they can be attributed to. Given sufficiently detailed data, even single devices like ovens, water boilers or washing machines can be identified from electricity measurements.[6] More recently, it has been shown that even watched TV programs[7] or the cup size of a coffee being prepared by a coffee machine[8] can under certain conditions be identified on the basis of highly resolved load graphs alone. The list of possible privacy invasions could be continued even further, but the general insight is already clear: Personal data about electricity consumption could possibly reveal deep insights into the personal habits of the respective customer. Beyond general concerns of the customer's fundamental rights having to be protected, such possible invasions might also result in significantly decreased acceptance of smart metering and thereby prevent the aspired goals from being actually accomplished.[9] The introduction of smart metering and smart grids must therefore be carefully examined in the light of data protection.[10]

This has, for instance, been done by the Article 29 Working Party of European data protection authorities, which concluded in 2011 that large portions of the data

[6] For vivid examples of what can, depending on the actual resolution, be deduced from household load graphs, see, for instance, Elias L. Quinn, "Privacy and the New Energy Infrastructure" (SSRN working paper, 2009), http://ssrn.com/abstract=1370731, accessed Nov. 28, 2011.

[7] See Ulrich Greveler, Benjamin Justus and Dennis Löhr, "Hintergrund und experimentelle Ergebnisse zum Thema 'Smart Meter und Datenschutz'," (technical report – V. 0.6 of Sept. 2011), http://www.its.fh-muenster.de/greveler/pubs/smartmeter_sep11_v06.pdf, accessed Nov. 28, 2011.

[8] See, for example, Gerald Bauer, Karl Stockinger and Paul Lukowicz, "Recognizing the Use-Mode of Kitchen Appliances from Their Current Consumption," *Smart Sensing and Context*, Lecture Notes in Computer Science, 2009, vol. 5741/2009, pp. 163–176, doi: 10.1007/978-3-642-04471-7_13.

[9] See, for instance, Layla AlAbdulkarim and Zofia Lukszo, "Impact of Privacy Concerns on Consumers' Acceptance of Smart Metering in The Netherlands," Proc. of the 2011 IEEE International Conference on Networking, Sensing and Control, Delft, pp. 287–292.

[10] As we will concentrate on the European perspective herein, we will use the term "data protection" in the following, referring to the nomenclature established by, for instance, the European data protection directive 95/46/EC and avoid the use of "privacy" which would possibly suggest a US-American perspective. Due to the significant differences with regard to the treatment of the respective aspects as well as in matters of market structure and regulation, a simple adoption of US-American models and approaches to smart metering and smart grids would hardly prove expedient within the scope of European regulations – an often overlooked fact that is unquestionably not restricted to data protection/privacy aspects alone.

that are to be collected and transmitted within smart metering environments have to be considered personal data as defined by the European data protection directive 95/46/EC and that the respective processes of collection, processing and use of these data therefore have to fulfill corresponding legal requirements.[11] On the other hand, the Article 29 Working Party also acknowledges that the landscape of smart meter legislation is in many respects "complex and disparate"[12] across Europe and that consistent regulations with regard to data protection in smart metering environments do not exist. At the moment, data protection issues of smart metering and smart grids can therefore only be discussed with regard to the general requirements as given by the data protection directive[13] or on the basis of the highly heterogeneous national legislation.

This notion coincides with that of the expert group focusing aspects of data protection within the "Task Force Smart Grids" established by the European Commission. As it is stated in the final report of this group, "[t]he current EU regulatory framework for smart metering […] insufficiently regulates the protection of privacy and personal data", thereby implying "a need for tailoring [smart metering approaches] down to a more concrete regulatory level […]."[14] Consequently, the expert group calls for the enactment of legal "provisions safeguarding the protection of privacy and personal data within smart metering [which] shall be of a uniform nature throughout the EU."[15]

In the light of this lack of a uniform, detailed European regulation with regard to data protection in smart metering and being well-aware of the nonetheless existing and possibly far-reaching implications of smart metering, the German legislator recently amended the national energy law in order to implement directive 2009/72/EC, to lay the groundwork for a broad establishment of smart metering and to foster the development of the above-mentioned functionalities within a smart grid.[16]

14.5 Energy Data Communication in Germany

An integral part of the recent amendment to German energy law consists of several regulations explicitly addressing data protection issues within smart metering environments. These regulations and the fundamental concepts underlying them shall be

[11] Article 29 Data Protection Working Party, "Opinion 12/2011 on Smart Metering."

[12] Article 29 Data Protection Working Party, "Opinion 12/2011 on Smart Metering," p. 4.

[13] A systematic analysis on the basis of the data protection directive was for example given by Rainer Knyrim and Gerald Trieb, "Smart metering under EU Data Protection Law," *International Data Privacy Law* 1(2, 2011), pp. 121–128, doi:10.1093/idpl/ipr004.

[14] Task Force Smart Grids – Expert Group 2, "Essential Regulatory Requirements and Recommendations for Data Handling, Data Safety, and Consumer Protection – Recommendation to the European Commission" (final draft of June 2011, p. 47), http://ec.europa.eu/energy/gas_electricity/smartgrids/doc/expert_group2_draft.pdf, accessed Nov 28, 2011.

[15] Task Force Smart Grids – Expert Group 2, "Essential Regulatory Requirements," p. 57.

[16] BGBl. I 2011, S. 1554, "Gesetz zur Neuregelung energiewirtschaftsrechtlicher Vorschriften."

discussed in the following. As, however, the energy sector is one of the most regulated areas within Germany as well as elsewhere across Europe, the existing status quo of energy data communication between the different market roles shall not be ignored but rather serve as a starting point for our deliberations. Before describing the newly introduced German approach, we will therefore give an overview of the established status quo of energy data communication in Germany and briefly introduce how energy data is communicated under a smart metering paradigm in two other countries: The Netherlands and the UK.

14.5.1 Status Quo of Energy Data Communication in Germany

In Germany, the local DSO is by default responsible for operating the metering points and for collecting measurement data. Different from other countries, the German customer may nonetheless assign another party, which might be her supplier as well as an independent third party, to be responsible for the operation of her metering point and the collection of the respective measurement data. To abstract from the different possible settings and to simplify matters, we will refer to an additional role of the *metering point operator (MPO)* in the following and ignore the question which party actually assumes this role.

The communication processes beginning with the MPO collecting measurement data from a meter are then specified by a rather complex set of laws, by-laws and specifications from regulatory agencies (especially the Federal Network Agency, Bundesnetzagentur). As we want to discuss data protection aspects herein, we can leave aside any processes regarding industrial customers and confine our considerations to those processes that refer to (potentially) personal data as defined in Art. 2, lit (a) of the directive 95/46/EC and thus regard private customers ("natural persons"). At a glance, measurement data from such private customers is in Germany currently communicated between the different market actors as follows:[17]

The MPO manually collects the measurement value from the customer (e.g. once a year) and transmits it to the local DSO. The DSO preprocesses and archives the received values, whereas the preprocessing especially includes checks for plausibility and, if necessary, the replacement of implausible values by plausible ones. From these long-term values and a well-defined set of "typical" load profiles, the DSO then generates an aggregated, high-resolution load-graph for every supplier and feeds these load-graphs into the balancing system, which is in Germany operated by the TSO. Furthermore, the DSO transmits the potentially preprocessed individual

[17] For a detailed description, see especially the documents BK6-09-034 – Wechselprozesse im Messwesen (change processes in measurement), BK6-06-009 – Geschäftsprozesse zur Kundenbelieferung mit Elektrizität (business processes for customer supply with electricity) and BK6-07-002 – Marktregeln für die Durchführung der Bilanzkreisabrechnung Strom (market rules for balancing electricity) given by the Federal Network Agency. All documents are available via http://www.bundesnetzagentur.de/

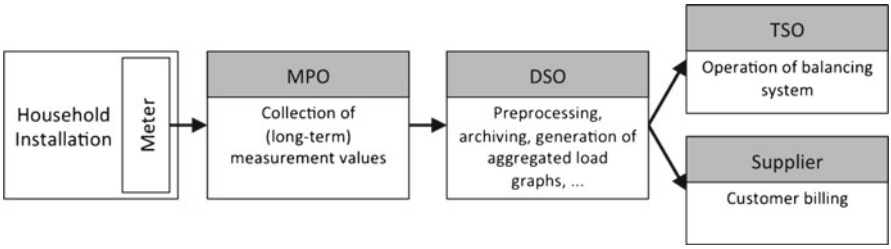


Fig. 14.1 Chained communication in the German electricity market

measurement values to the supplier who bills his customers on this basis. The underlying paradigm of "chained communication" can be visualized as done in Fig. 14.1.

Due to the fact that measurement values have up to now referred to rather long periods and were collected and transmitted by the MPO once a year or, in some cases, on a monthly basis, data protection issues with regard to the collection, processing and transmission of energy-related consumption data played no significant role. The resulting infringements of data protection rights were insignificant and the data were unquestionably necessary for carrying out the supply of the customer with electricity and for operating the unbundled, liberalized electricity market. This is, however, not the case anymore with the high-resolution data potentially being collected, processed and used within smart metering environments.

14.5.2 Excursus: Smart Meter Communication in the Netherlands and the UK

Before going into the details of Germany's current smart meter legislation, we will briefly outline the approaches pursued in two other European Countries in order to provide further context for the subsequent deliberations and to highlight the distinctive characteristics of the German approach. In this respect, the Netherlands and the UK are particularly noteworthy.

14.5.2.1 Smart Meter Communication in the Netherlands

As the Netherlands' initiative for establishing smart metering gained significant attention in the past, the approach pursued there shall be depicted in brief. Originally, the installation and use of smart meters was planned to be compulsory in the Netherlands, but after severe protests, consumers now have the right to refuse.[18]

[18] In fact, the customer has four different graded options between "refuse" and "full use". See Stephan Renner et al., "European Smart Metering Landscape Report," pp. 53 ff., 59 f.

When not refused, smart meters are installed and operated by the respective local DSO. Different from Germany, consumers can not voluntarily change to a third party for operating and reading out measurement data.[19]

Measurement data is collected by the DSO via secure channels and fed into a "central system (CS)". From here, it flows to the operational units of the DSO, to the respective supplier, to the party responsible for operating the balancing system (which is in the Netherlands in most cases done by suppliers or traders) and possibly to independent service operators.[20] The general communication model is thus one of "chained communication" and does to a certain extent resemble the established German model outlined above.

The meters themselves have to provide two different tariff registers for rather simple tariff models diversifying between on- and off-peak hours alone.[21] By default, meters are read out once every 2 months. With the customer's explicit permission, meter readings can however be collected in different intervals,[22] whereas the meter itself collects one value for any 15-min-interval.[23] The communication model thereby supports rather complex and dynamic tariffing schemes to be realized in the backend.

Beyond the fact that the DSO has to employ usual security mechanisms for secure remote reading and for restricting access to data from the CS for the different parties retrieving it, no explicit means of normatively determined technical data protection are apparent within the approach pursued in the Netherlands.

14.5.2.2 Smart Meter Communication in the UK

The approach to smart metering pursued in the UK is noteworthy because of the unique construct of a single, nationwide "data and communications company

[19] See Netbeheer, "Dutch Smart Meter Requirements," (V. 4.0 of April 2011), http://www.energiened.nl/_upload/bestellingen/publicaties/284_313185a%20-%20DSMR%20v4.0%20final%20Main.pdf, accessed Nov. 28, 2011, p. 51: "Only the grid operator shall have direct access to the metering installation via the [external interface … He] is also responsible for the correct data communication from the metering installation to the central system and vice versa."

[20] See Energie-Nederland, "Energie in Nederland 2011 – Energy in the Netherlands 2011" (2011, pp. 16, 80), http://www.energie-nederland.nl/wp-content/uploads/2011/08/Energie-in-Nederland-2011.pdf, accessed Nov. 28, 2011. For the general communication structure, see also the figure in Netbeheer, "Dutch Smart Meter Requirements," p. 10 or Layla Al Abdulkarim and Zofia Lukszo, "Smart Metering for the Future Energy Systems in the Netherlands" (paper presented at the Fourth International Conference on Critical Infrastructures, Linkoping, 2009).

[21] See Netbeheer, "Dutch Smart Meter Requirements," p. 17.

[22] See Stephan Renner et al., "European Smart Metering Landscape Report," p. 53.

[23] See Netbeheer, "Dutch Smart Meter Requirements," pp. 61 f., 68 f.

(DCC)". Basically, the suppliers are obligated to install smart meters at their customers' sites[24] while the collection of measurement data via secure channels and its provision to the different actors within the liberalized and unbundled market shall entirely be done by the (to be established) DCC. Data provision shall be subject to technical access restrictions applied by the DCC and it is explicitly aspired that customers should be able to allow third parties to access their measurement data via the DCC, too.[25]

With regard to data protection, the general rule is that "[c]ustomers will have a choice over how their consumption data is used and by whom, except where data is required to fulfil regulated duties."[26] Approaches for minimizing the amount of collected and processed personal data by means of privacy enhancing technologies are rudimentarily discussed, but no explicit specifications have been made yet.[27] Similarly, it is also not yet specified in what resolution measurement data will be sent to the DCC and which data shall be deemed "required to fulfill regulated duties", therefore necessitating no consent to be given by customers.[28] Like in the Netherlands, smart meters will have a limited number of registers for realizing rather simple tariff schemes distinguishing between on- and off-peak consumption,[29] while more complex and dynamic tariffs will have to be realized in the backend on the basis of more highly resolved consumption data.

It is, however, not yet conceivable how access restrictions shall actually be realized within the DCC and what technical measures beyond this access restriction and the secure transfer between meter and DCC will actually be employed. Further technical mechanisms for enhancing customers' data protection rights before measurement data accumulates in the DCC are not evident.

---

[24] See Stephan Renner et al., "European Smart Metering Landscape Report," p. 88.

[25] See DECC, "Smart Metering Implementation Programme: Response to Prospectus Consultation – Supporting Document 1 of 5 – Data Access and Privacy," (2011, p. 22), available via http://www.decc.gov.uk/, accessed Nov. 28, 2011.

[26] DECC, "Smart Metering Implementation Programme: Response to Prospectus Consultation – Overview Document," (2011, p. 3), available via http://www.decc.gov.uk/, accessed Nov. 28, 2011.

[27] See, in particular, DECC, "Smart Metering Implementation Programme: Response to Prospectus Consultation – Supporting Document 1 of 5 – Data Access and Privacy," p. 10.

[28] This question is also subject to a recent call for evidence to broaden the basis for the DECC's rulemaking. See DECC, "Smart Metering Implementation Programme: A call for evidence on data access and privacy," (2011), available via http://www.decc.gov.uk/, accessed Nov. 28, 2011. The underlying vagueness was also objected by Ross Anderson, Shailendra Fuloria and Éireann Leverett, "Data Privacy and Security for Smart Meters – Response to Ofgem's Consultation," (2011, p. 2 f), http://www.cl.cam.ac.uk/~rja14/Papers/DECC-sm-final.pdf, accessed Nov. 28, 2011.

[29] See DECC, "Smart Metering Implementation Programme: Response to Prospectus Consultation – Overview Document," p. 25.

14.5.3 Smart Meter Legislation in Germany

In order to comply with the requirement for widespread adoption of smart metering arising from the "electricity directive" 2009/72/EC,[30] the amended German energy law (Energiewirtschaftsgesetz, EnWG) introduces the new term of a "measurement system" and defines it as a "measurement device […] that is integrated into a communication network".[31] Furthermore, the energy law declares that such measurement systems have to be installed by the respectively responsible MPO in new or substantially renovated buildings, at final customers with an overall consumption of more than 6,000 kWh/year and in some specific cases of privately owned renewable or combined heat and power (CHP) generation units whenever this is "technically feasible". In all other cases, measurement systems have to be installed whenever this is technically feasible and "economically justifiable". In the end, the installation of such measurement systems will become obligatory to a multitude of private final customers as soon as legally compliant systems are available on the market, and for nearly all private final customers for the potential case of the economic feasibility being declared within a subordinate by-law or when electronic measurement systems actually turn out to raise no additional costs for the final customer.[32]

14.5.4 The German Approach to Data Protection in Smart Metering Environments

Like in many other European countries, data protection considerations played a major role during the legislation process related to the introduction of smart metering. Being highly aware of the potential risks that could arise from the introduction of smart metering, the German legislator therefore involved data protection authorities as well as the Federal Agency for Information Security into the legislation process from the very beginning. In the end, this resulted in a specific German approach to data protection in smart metering environments.

---

[30] See, for instance, 2009/72/EC, Annex II, Nr. 2: "Member States shall ensure the implementation of intelligent metering systems that shall assist the active participation of consumers in the electricity supply market. The implementation of those metering systems may be subject to an economic assessment of all the long-term costs and benefits to the market […]. Where roll-out of smart meters is assessed positively, at least 80% of consumers shall be equipped with intelligent metering systems by 2020."

[31] See § 21d EnWG: "Ein Messsystem im Sinne dieses Gesetzes ist eine in ein Kommunikationsnetz eingebundene Messeinrichtung zur Erfassung elektrischer Energie, das den tatsächlichen Energieverbrauch und die tatsächliche Nutzungszeit widerspiegelt."

[32] The latter condition depends on a multitude of factors, including the price of the device itself, the costs of its operation or even the business model of the MPO. It is therefore hard to provide well-founded estimations about the implications of this legally set precondition at the moment.

At the heart of this German approach lies the establishment of absolute "data sovereignty" being exerted by customers over their measurement data. The term "data sovereignty" had previously been unknown within German data protection legislation but during the legislation process, it was defined by the government as the customer's "exclusive right of decision over the use of consumption data from her intelligent meter,"[33] implying that nobody shall have access to the respective data without the customer's explicit consent and that the customer should always be in full control of any transfer of measurement data.

Furthermore, the principle of data minimization formed another precept for the implementation of smart metering in Germany, implying that the collection, processing and use of personal data should be limited to the absolutely required minimum. Together, the concepts of data sovereignty and data minimization formed the starting point for a German approach to smart metering that should implement the concept of "privacy by design" or "smart privacy"[34] as far as possible.

From an early point of development, there was broad consensus that additional technical requirements have to be prescribed with regard to the devices installed at the customer's site in order to ensure a level of technical data protection that meets German aspirations.[35] As it would, however, have conflicted with the rules of the internal European market to raise additional technical requirements for electronic meters beyond those harmonized on the European level,[36] an additional technical entity had to be introduced that is distinct from the meter itself and that realizes those functions deemed necessary from the national point of view: the "smart meter gateway".

---

[33] Freely translated from Bundestag, "Entwurf eines Gesetzes zur Neuregelung energiewirtschaftsrechtlicher Vorschriften" (BT-Drucks. 17/6248), p. 4. In original: „[Der Gesetzentwurf] weist ihm alleine die Bestimmung über die Verwendung von Verbrauchsdaten seines intelligenten Zählers zu […]."

[34] See Ann Cavoukian, Jules Polonetsky and Christopher Wolf, "SmartPrivacy for the Smart Grid: embedding privacy into the design of electricity conservation," *Identity in the Information Society* 3 (2010), pp. 275–294, doi: 10.1007/s12394-010-0046-y.

[35] Similar implications were also derived from deliberations on overall system security within the electricity grid and the need for an appropriate protection against malicious attacks possibly involving those entities installed at the customers' side. In this respect, see, for example, Himanshu Khurana, Mark Hadley, Ning Lu, and Deborah A. Frincke, "Smart-Grid Security Issues," *IEEE Security & Privacy* 8 (1, 2010), pp. 81–85; Patrick McDaniel and Stephen McLaughlin, "Security and Privacy Challenges in the Smart Grid," *IEEE Security & Privacy* 7 (3, 2009), pp. 75–77; Ivan L.G. Pearson, "Smart grid cyber security for Europe," *Energy Policy* 39 (9, 2011), pp. 5211–5218; Claudia Eckert, "Sicherheit im Smart Grid" (Alcatel-Lucent-Stiftung, 2011) http://www.stiftungaktuell.de/files/sr90_sicherheit_im_energieinformationsnetz_gesamt.pdf, accessed Nov. 28, 2011. We will, however, mainly concentrate on those aspects related to data protection in the following.

[36] On the European level, technical requirements for meters – or rather "measurement devices" – are harmonized through the "Measurement Instruments Directive (MID)" 2004/22/EC. With regard to "smart meters", harmonizing European regulations are currently developed under Mandate 441. See European Commission, "Standardisation mandate to CEN, CENELEC and ETSI in the field of measurement instruments for the development of an open architecture for utility meters involving communication protocols enabling interoperability," (M/441, 2009), http://ec.europa.eu/energy/gas_electricity/smartgrids/doc/2009_03_12_mandate_m441_en.pdf, accessed Nov 28, 2011.

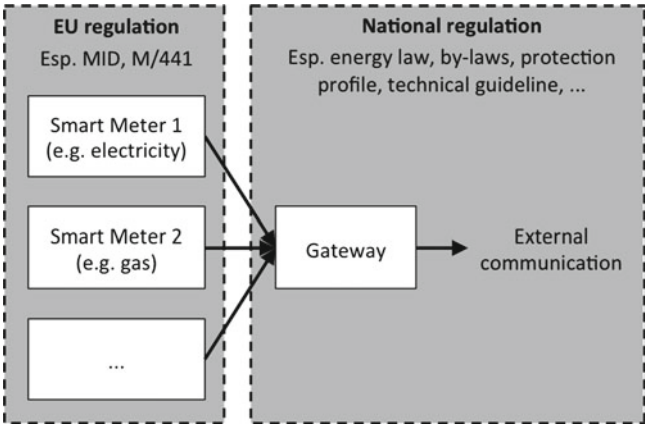


Fig. 14.2 Scope of European and national regulation in the German model

The requirements having to be fulfilled by this smart meter gateway in order to form a legally compliant measurement system together with a usual electronic meter will be defined in additional by-laws as well as in protection profiles and technical guidelines that are to be established by the German Federal Office for Information Security (Bundesamt für Sicherheit in der Informationstechnik, BSI) in cooperation with the Federal Network Agency as the national regulatory authority and the Physical-Technical Federal Agency (Physikalisch-Technische Bundesanstalt, PTB) as the national metrology institute.[37] The protection profile, which had been initiated in late 2010, was finalized in August 2011,[38] and the technical guideline was available in a first draft version in late 2011.[39]

Altogether, this boils down to a modular measurement system where one or more electronic meters falling within the scope of European regulation are connected to a "smart metering gateway" falling within the scope of national legislation (see Fig. 14.2). The detailed legal as well as technical elaboration of the German data protection framework for smart metering then rests upon four main concepts. These are:

- a paradigm of star-shaped *end-to-end communication between gateway and market actors*, replacing the established concept of chain-formed communication,
- mainly local storage of measurement data with access being granted to the different market actors on the basis of *locally enforced, receiver-specific access profiles,*

[37] See §§ 21e, 21i EnWG.

[38] See BSI, "Protection Profile for the Gateway of a Smart Metering System" (V 1.1.1 final draft, 2011, in the following: BSI-PP), available via https://www.bsi.bund.de/DE/Themen/SmartMeter/Schutzprofil/schutzprofil_node.html, accessed Nov. 28, 2011.

[39] See BSI, "TR-03109: Anforderungen an die Interoperabilität der Kommunikationseinheit eines intelligenten Messsystems für Stoff und Energiemengen" (V 0.2.0 draft, 2011, in the following: BSI-TR), available via https://www.bsi.bund.de/DE/Themen/SmartMeter/TechnRichtlinie/TR_node.html, accessed Nov 28, 2011.

- different kinds of *local preprocessing of measurement data* being executed on the gateway before sending data to external parties, including local tariffing, and, finally,
- a *complete ex-ante definition of legitimate data uses* given in national energy law, declaring any collection, processing and use of personal data from the measurement system beyond this set of data uses illegitimate.

In order to allow for a well-founded discussion of the German approach to energy data communication, these foundational main concepts shall be laid out in more detail.

14.5.4.1 Main Concept 1: End-to-End Communication Between Gateway and Market Actors

The most fundamental – and presumably most far-reaching – concept underlying the German approach to data protection in smart metering environments regards the assumed communication paradigm. Different from the established chain-formed communication model outlined above and also pursued for smart metering in the Netherlands and the UK, the German approach to smart metering basically assumes a model of star-shaped end-to-end communication where multiple parties communicate (more or less) directly with the smart meter gateway.

In particular, § 21g of the amended energy law explicitly declares the MPO, the network operator (which includes the DSO as well as the TSO), the supplier and any additional party being able to provide the written consent of the customer as being authorized for the collection, processing and use of personal data from the measurement system. This declaration only makes sense under the assumption that the mentioned parties actually collect data directly from the gateway instead of receiving it within chain-formed downstream processes.

The underlying concept of different external entities communicating directly with the gateway is also illustrated by the protection profile, which explicitly assumes that data from the connected meters is submitted to different external parties depending on different access control profiles. These access control profiles, in turn, shall be used for receiver-specific definition of the preprocessing that is to be done before submission, of the key material that is to be used for encryption and signing, whether data should be pseudonymized, etc.[40] Again, such declarations only make sense under the assumption of multiple external parties communicating directly with the meter gateway.

[40] See BSI-PP, line 317 ff. In this respect, see also BSI-PP, line 478 ff ("the data can only be read by the intended recipient and only contains an association with the identity of the Meter if this is necessary.") as well as the cardinality of "1…n" authorized external entities in BSI-PP, line 196, figure 2.

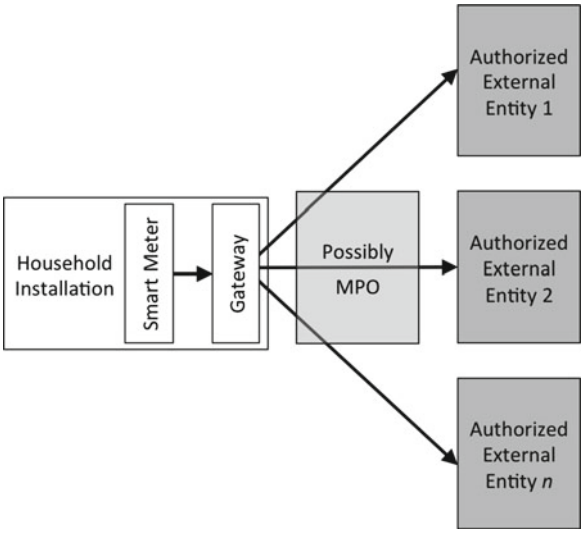


Fig. 14.3 Star-shaped end-to-end communication model underlying German legislation

This general conclusion also holds true in the light of the "mediated direct communication" to external parties envisaged within the protection profile as well as in the technical guideline. Such mediated direct communication employs two-layer cryptography (content and channel) and especially refers to cases where "the external party that the [gateway] communicates with is not the final recipient of the Meter Data."[41] In particular, this option has been established to allow for practices where any data is always sent to the MPO who then forwards it to the respective external party without being able to gain knowledge about the actual content of transmitted data. Furthermore, such mediated direct communication is also necessary to realize actual pseudonymization as in the case of non-mediated direct communication, the respective external party would always know where the received pseudonymized data originates from, thereby rendering any pseudonymization useless.[42]

Even with the possibility of the MPO (or another party) being employed as mediating instance, the fundamental communication concept underlying German regulations for smart meter communication is thus still one of star-shaped end-to-end communication taking place between a smart meter gateway and different authorized external entities whereas the consumers' data protection rights are to be technically safeguarded by means of receiver-specific end-to-end encryption and pseudonymization. Figure 14.3 visualizes this communication concept.

[41] BSI-PP, line 545 f.

[42] This use case is, for example, explicitly discussed in BSI-TR, line 411 ff.

14.5.4.2 Main Concept 2: Local Storage and Execution of Access Profiles

Strongly bound to the concept of direct end-to-end communication between gateway and the different market actors is the concept of locally stored and executed, receiver-specific access profiles. As already mentioned above, these access-profiles define which data is to be submitted to which external party in which intervals after what kind of preprocessing using what key material for encryption and signing etc. The fundamental recognition behind this receiver-specific communication is that measurement data is needed in different forms and for different purposes by the different market actors. The supplier, for instance, must be able to bill his customers on the basis of the highly dynamic tariffs outlined in Sect. 14.3 above and needs the data that is necessary for doing so. The DSO may have a need for knowing the total aggregated load or the voltage within a given network segment in near real-time for the purpose of network monitoring but may at the same time have no need for knowing this data in individualized, customer-specific form. The TSO, in turn, may have a need for highly resolved data aggregated over all customers of a given supplier for managing the above-mentioned balancing mechanism but will, like the DSO, have no reasonable need for individualized data.[43]

The approach pursued with the local storage and execution of receiver-specific access profiles is, then, to restrict the data that is transferred to the absolute minimum as defined by these "data needs", thereby implementing the above-mentioned principle of data minimization. The principle of data sovereignty, in turn, assumes that this data flow control necessarily has to take place within the local sphere of the customer. Only with physical control over the device that applies the access profiles, the argument goes, can the customer be confident that no additional access or transfer happens beyond those defined within the access profiles. While access restrictions for the different market actors are to be applied in some sort of backend system in the Netherlands as well as in the UK, this shall be done locally on the smart meter gateway in Germany.

14.5.4.3 Main Concept 3: Local Preprocessing of Measurement Data and Local Tariffing

Besides the restriction of access to locally stored data and the specification of the encryption and/or pseudonymization methods that are to be used for data transmission, the protection profile also requires that access profiles allow for the specification of preprocessing functions that are to be applied to measurement data before transmission.[44] Even if no further details for this preprocessing functionality have been

[43] For a more detailed but still not exhaustive depiction of the different "data needs", see, for instance, Frank Pallas, "Data Protection and Smart Grid Communication – The European Perspective," Proc. of the 2012 IEEE PES Innovative Smart Grid Technologies Conference, doi: 10.1109/ISGT.2012.6175695.

[44] See BSI-PP, line 321f.: "An access profile defines how meter data must be processed […]."

explicitly specified so far, explanatory publications by representatives of the federal data protection authority as well as of the BSI do at least suggest that this mechanism shall particularly be employed to address a postulation that data protection authorities and other parties have made from the very beginning: that of local tariffing on the basis of highly dynamic, possibly weather-dependent prices without a need for detailed measurement data being sent to the supplier's backend systems.[45] Put briefly, "the gateway itself shall be able to perform the necessary tariffing."[46]

This local tariffing shall be realized by means of supplier-specific access profiles defining that no detailed measurement data may be accessed but that measured data are to be attributed to or even multiplied by the respectively relevant price as defined within a previously transferred tariff profile instead. Within rather simple schemes that only distinguish between on- and off-peak hours, this could easily be done by summing up all consumption amounts for each tariff level and by submitting aggregated values for each price level once in a month, comparable to the method of different registers as envisaged in the Netherlands and the UK. Under the conditions of the highly dynamic tariff schemes that are explicitly aspired with the introduction of smart grids,[47] however, such local tariffing will necessarily require comparably complex calculations to be executed locally by the smart meter gateway. Different from the Netherlands and the UK, the gateway would then merely report a total invoice amount to the supplier.

In the end, local tariffing (and possibly further kinds of local preprocessing) shall render the transmission of detailed, individualized measurement data to external parties dispensable and thus prevent the respective parties from gaining any knowledge about customer-specific consumption- and thus behavior-patterns.[48] The underlying concept of (partially) relocating data processing from backend systems onto the smart meter gateway therefore addresses the fundamental principle of data minimization.

14.5.4.4 Main Concept 4: Complete Ex-ante Definition of Legitimate Data Uses

The fourth main concept that shall be discussed herein does not originate from the technical or the techno-legal but rather from the purely legal domain. As already noted above, § 21g of the amended energy law explicitly declares the MPO, the network operator (which includes the DSO and the TSO), the supplier and any

[45] Such postulations have, amongst many others, been made by Dennis Laupichler, Stefan Vollmer, Holger Bast and Matthias Intemann, "Das BSI-Schutzprofil," *Datenschutz und Datensicherheit – DuD* 8/2011, p. 544 (speaking for the BSI); Klaus J. Müller, "Verordnete Sicherheit – Das Schutzprofil für das Smart Metering Gateway" *Datenschutz und Datensicherheit – DuD* 8/2011, p. 551; or Eckert, "Sicherheit im Smart Grid," p. 31.

[46] Pfändler, "Smart Meter und Smart Grid", p. 5 (speaking for the federal data protection authority). In original: "die Kommunikationseinheit [soll] in der Lage sein, die notwendige Tarifierung selbst vorzunehmen."

[47] See Sect. 14.3 above.

[48] See Sect. 14.4 above.

additional party being able to provide the written consent of the customer as being authorized for the collection, processing and use of personal data from the measurement system. Furthermore, § 21g also provides that the collection, processing and use of personal data from the measurement system is only legitimate insofar as this is necessary for:

- The constitution, content-forming and change of a contract by request of the customer
- The measurement of energy consumption and feed-in
- The supply with energy including the billing
- The feed-in of energy including the billing
- The control of specific types of interruptible appliances (as further defined in other paragraphs of the energy law)
- The realization of dynamic tariffs (as further defined in other paragraphs of the energy law)
- The detection of the current network situation in justified and documented exceptional cases
- The detection or prevention of fraud.

This enumeration of legitimate purposes has to be deemed exhaustive, implying that no further purposes can be legitimated on another basis like the customer's explicit consent or the unambiguous vital interest of the customer as it is provided by general German data protection law (BDSG) or even in Art. 7 of the European Data Protection Directive 95/46/EC.[49] Different from established conceptions of general data protection regulations, and different from the Netherlands and the UK, where the customer shall be able to define data receivers without apparent restrictions, § 21g of the amended German energy law thus defines a complete, exhaustive set of legitimate data uses ex-ante and declares any data use beyond this well-defined set illegitimate.[50]

14.5.5 Synopsis

Altogether, the German approach to data protection within smart metering environments pursues the explicitly stated goal of establishing an energy customer's "data

[49] This notion is also supported by the German government which explicitly stated that the catalogue of legitimate purposes shall be deemed exhaustive and that the collection, processing and use of data from the measurement system shall *solely* be legitimate for the cases explicitly mentioned in the catalogue. See Bundesrat, "Entwurf eines Gesetzes zur Neuregelung energiewirtschaftsrechtlicher Vorschriften," (BR-Drucks. 343/11), p. 202: "§ 21g legt in Absatz 1 einen abschließenden Katalog von Fällen fest, in denen die Erhebung, Verarbeitung und Nutzung personenbezogener Daten zulässig ist."; p. 196: "Erhebung, Verarbeitung und Nutzung personenbezogener Daten sind ausschließlich in den in § 21g beschriebenen Fällen zulässig […]."

[50] For a slightly more exhaustive discussion on this issue, see Oliver Raabe, Mieke Lorenz, Frank Pallas and Eva Weis, "Harmonisierung konträrer Kommunikationsmodelle im Datenschutzkonzept des EnWG," *Computer und Recht*, 12/2011, pp. 831–840.

sovereignty" over "her" personal data, implying that the customer shall have full control over any use of consumption data from her intelligent meter. The second goal pursued by the German approach is that of data minimization, which is a well-known principle of data protection and refers to the restriction of data collection, processing and use to the smallest possible amount. Only data that proves absolutely essential shall be communicated to external parties.

These overarching aims are addressed through a combination of legal and techno-legal instruments within German energy legislation, of which the most important is the introduction of an additional technical entity – the smart meter gateway – that is employed for establishing advanced technical prerequisites which cannot be allocated to the meter because of European regulation. Aside from the main concept of complete ex-ante definition of legitimate data uses, further legislation with regard to data protection mainly refers to this smart meter gateway: The smart meter gateway communicates (even if possibly in mediated form) directly with the different external entities and any external entity receives data as defined within a receiver-specific access profile that is applied locally on the gateway to ensure the customer's full control over the transfer and thus the use of her personal data. Access profiles should also be used to determine receiver-specific encryption and pseudonymization methods and even more complex preprocessing functions that are to be applied to the data before being transmitted to the respective external entity. As the given and explicitly aspired use-case of local tariffing shows, these functionalities serve the overall goal of data minimization.

The German approach to energy data communication thus significantly differs from the ones pursued in the Netherlands and the UK. In particular, the differences refer to mechanisms that have been introduced in Germany to address different aspects of data protection in a vein that follows the concept of "privacy by design" or "smart privacy" as far as possible.

Unquestionably, the now compulsory mechanisms were strongly inspired by those approaches that are rightly regarded as state of the art for technical data protection within the field of internet-based communication. Only with technical measures of data flow control and data minimization being realized on the end hosts can the "right to informational self-determination", which was declared as fundamental right by the German Federal Constitutional Court in 1983,[51] effectively be implemented under the conditions of communication being carried out over an untrustworthy, per-se hostile medium like the internet. Intuitively, the German approach to data protection within smart metering environments therefore sounds highly plausible. What has proven expedient for internet-based communication in the past must be right for the so-called "internet of energy"[52] as well.

[51] See BVerfGE 65, 1.

[52] See, for instance, BDI, "Internet of Energy – ICT for Energy Markets of the Future – The Energy Industry on the Way to the Internet Age," (BDI publication No. 439, 2010) http://www.bdi.eu/bdi_english/download_content/ForschungTechnikUndInnovation/BDI_initiative_IoE_us-IdE-Broschure.pdf, accessed Nov 28, 2011. See also Sean Davies, "Internet of Energy," *Engineering & Technology* 5 (16, 2010), pp. 42–45.

14.6 Critical Discussion

A thorough examination of the actual givens within the German energy market as well as of the main foundational concepts does, however, reveal a number of shortcomings that render the German approach to data protection within smart metering environments less convincing. As we will see, some of the now established regulations can only be explained by a nonconsideration of the actual givens from the energy sector while others suggest a questionable conception of "self-determination" with regard to personal data. Altogether, this raises the concern of energy-related data protection legislation being – at least to a certain extent – created from a gut level and not on the basis of diligent and well-informed deliberations in Germany. To highlight the existent shortcomings and to prevent them from being repeated during a potential adoption of the German approach either in other national legislations or even on the European level, the above-mentioned main concepts shall thus be subject to a critical discussion. We will do this in reverse order, starting with the complete ex-ante definition of legitimate data uses.

14.6.1 Complete Ex-ante Definition of Legitimate Data Uses: Discussion

The ex-ante definition of a well-defined and exhaustive set of external parties and, in particular, legitimate purposes for the collection, processing and use of personal data from the smart meter was established to protect the energy customers' fundamental right for informational self-determination.[53] By restricting data uses from the outset, any attempt to establish further "uncontrolled" data flows later shall be forestalled preemptively, thereby protecting the customer from her data being misappropriated.

A closer inspection does, however, reveal that even the now-established form prohibits the collection, processing and use for further purposes beyond those explicitly mentioned even if the customer has explicitly given her consent. Instead of actually serving the goal of self-determination – which would unquestionably also include the self-determined permission of access to any self-chosen external party for any self-chosen purpose – the German lawmaker has thus in fact paternalistically restricted the informational self-determination of energy customers to those cases actually foreseen and deemed acceptable by the lawmaker himself.

This seems questionable not only in general but also with regard to the future development of innovative, not yet foreseeable services that do not involve explicit contracts being closed by the customer and that may thus not be legitimated by the

[53] See Bundesrat, "Entwurf eines Gesetzes zur Neuregelung energiewirtschaftsrechtlicher Vorschriften," p. 202: "[Die] Vorschriften dienen in zentraler Weise dem Schutz des Grundrechts auf informationelle Selbstbestimmung […]."

"constitution, content-forming and change of a contract by request of the customer". While such services could, for example in the form of collaborative energy efficiency networks,[54] play an important role for the improvement of energy efficiency within the smart grid and thereby serve the overall societal goal of climate protection, the German regulations in the current form would prevent them from being actually established – even if customers themselves would like to participate in such networks.

Going one step further, it can be stated that as compared to the other explicitly mentioned purposes, the first purpose of data being collected for the "constitution, content-forming and change of a contract" is formulated rather broadly, thereby opening the use of energy-related data to a multitude of contractual relations that might even lie far beyond the energy field. This was for example criticized by the Independent Center for Data Protection of Schleswig-Holstein during the legislation process, arguing that this option would unnecessarily soften the otherwise strong purpose limitation and should therefore be discarded.[55]

In the light of the above-mentioned fact that the catalogue of explicitly mentioned purposes has to be deemed exhaustive, such a deletion would have had far-reaching implications. In the end, it would have prohibited any use of the respective data within business models that are not explicitly declared legitimate in the energy law and, in particular, those business models that do not belong to the core energy market, even if there were a contractual relation between the customer and the party offering a certain service. This would have even tightened the limitations of informational self determination already present in the now-established version of the German energy law. By now, however, this strengthening did not make its may into the enacted energy law.

We can thus conclude that the explicit and exhaustive definition of legitimate purposes actually restricts the individual customers' informational self-determination to those use cases already foreseen today. Innovative uses of measurement data may therefore contradict with the now-established German energy law and would thus prove illegitimate from today's point of view. The strict ex-ante confinement to a well-defined set of purposes may then turn out to be a hindrance for innovation, individual benefit, and even energy efficiency. It is not clear whether the lawmaker was aware of these implications or to what extent they were actually subject to conscious deliberations during the lawmaking process.

Besides those aspects of direct practical relevance, the exhaustive ex-ante definition of legitimate purposes also gives room for more general discussions.

---

[54] See, for example, Andreas Kamper and Anke Eßer, "Strategies for Decentralised Balancing Power," in Andrew Lewis, Sanaz Mostaghim and Marcus Randall (ed.), *Biologically-Inspired Optimisation Methods,* Studies in Computational Intelligence, 2009, Volume 210/2009, pp. 261–289, doi: 10.1007/978-3-642-01262-4_10.

[55] See Independent Center for Data Protection Schleswig-Holstein, "ULD-Stellungnahme zur Smart-Meter-Regelung im Rahmen der Energiewende," (2011, p. 3) https://www.datenschutzzentrum.de/smartmeter/20110615-smartmeterregelung.pdf, accessed Nov. 28, 2011.

Strictly speaking, the approach of preventing customers from granting access to their energy data to any party and for any purpose on the basis of their own free will does, even if unquestionably well-intentioned by the legislator, constrain individual self-determination. This might be interpreted as an act of governmental paternalism motivated by data protection considerations, thereby raising a whole new class of questions for further discussion.

We will, however not address these questions in more detail but rather pass on to the next main concept: the local preprocessing of measurement data and local tariffing.

14.6.2 Local Preprocessing and Local Tariffing: Discussion

As outlined above, the concept of local preprocessing of data is at the moment mainly discussed with regard to the local tariffing on the basis of dynamic prices without transferring high-resolution measurement data to external parties like the supplier. Unquestionably, this would very well serve the overarching goal of data minimization. The local preprocessing was therefore a key postulation of German data protection authorities and activists.[56]

Up to now open is, however, the question how the "data needs" of further actors beyond the supplier should be fulfilled in this model. As outlined in Sect. 14.2, for example, network operators like the DSO and the TSO have to be strictly separated from the supplier within a liberalized, unbundled market. In order to get paid for the maintenance of their networks, these network operators also must be able to perform their billing in accordance with the respective national legislation. At least in Germany, network operators usually bill the supplier for using their network to transport and distribute electricity from the generation point to the customer. With regard to private customers, this is currently in most cases done on the basis of the overall amount of electricity being delivered. At least this case must also be supported within smart metering environments. Within the established model, this could simply be done by reporting an overall consumption value from the gateway to the respective network operator.

There is, however, a certain probability that private customers' network fee will in the future depend on further factors beyond overall consumption. Corporate customers, for instance, do in many cases already pay a fee that also depends on the maximum load within a certain interval today. This practice might very well be

[56] On a European level, a comparable notion was also made by the Task Force Smart Grids – Expert Group 2, "Essential Regulatory Requirements and Recommendations for Data Handling, Data Safety, and Consumer Protection," p. 42, stating that the purpose of billing and payment only requires "summed up usage".

applied to private customers too.[57] In analogy to the above-mentioned concept of dynamic, weather-dependent prices, network fees could in the medium term also be made dynamic to reduce network load during peak periods. Should such ideas actually gain momentum, the calculation of network fees would under the paradigm of local preprocessing also have to be realized locally, introducing yet another need for conducting local calculations on high-resolution data.

A further ambiguity related to the billing process regards the strongly associated process of balancing. As already noted in Sect. 14.3, the intentional adoption of consumption behavior to the current, e.g. weather-dependent generation by means of highly dynamic prices requires real (aggregated) measurement values to be fed into the balancing mechanism. Without such a feedback of actually changed consumption into the balancing mechanism, the supplier would have no incentive to actually offer dynamic prices and in the end, this would render all price-based approaches for a better integration of fluctuating sources of generation (especially wind, PV) foredoomed. While the use case of the supplier having to bill his customers was explicitly addressed in the German model, this indispensable need for feeding back actual measurement data into the balancing mechanism was largely overlooked during the specification process of the protection profile and, at least so far, the technical guideline. Like the question for the billing of network fees, the highly important question whether and how such a feedback mechanism could fit into the concept of data being to a large extent preprocessed locally on the gateway is thus not even rudimentarily answered. We will return to this problem in Sect. 14.6.3 below.

We can therefore state that the strong focus on relocating large portions of the billing process between supplier and customer onto the local gateway is by large not sufficient for establishing the concept of data minimization within the energy market as long as other indispensable processes are not addressed properly. It can only be speculated about why the former got significant attention during the German legislation process while the latter did not. The observable status quo from protection profile as well as technical guideline does, however, raise concerns of the actual givens and necessities within a liberalized, unbundled electricity market not having been adequately incorporated during the specification process. It might be the case that some of the currently existing lacks could indeed be dispelled within the paradigm of strong local data processing, but the current absence of concrete specifications or even deliberations does at least introduce uncertainties with regard to the future structure of well-established core processes of the energy market.

[57] In fact, the calculation model for the network fee does in Germany depend on the measurement method being employed. The mentioned calculation that is also based on the maximum load applies to customers measured by “load profile measurement”. The amended energy law, in turn, authorizes the federal network agency to specify a specific measurement method for smart meters “as a special form of load profile measurement” (§21i, 1, no. 7 EnWG). In this case, the calculation of network fees would consequently have to be realized under the model that incorporates the maximum load.

This is also the case with regard to the remaining concepts of local data flow control and star-shaped end-to-end communication between the gateway and the different external parties. These two concepts underlying the German approach to smart energy data communication can not be strictly separated from each other and we will therefore discuss them conjointly.

14.6.3 Star-Shaped Communication and Local Data Flow Control: Discussion

The concepts of star-shaped end-to-end communication and local data flow control are primarily aimed at the goal of establishing "data sovereignty" and thus of giving the customer full control over the collection and use of her measurement data. With regard to the well-known case of internet communication, these concepts are for good reasons seen as the only practical approach for ensuring informational self-determination, as everything happening beyond the local device practically eludes the actual exertion of control. With regard to the electricity system, however, this does not necessary hold true. Instead, the strict assumption of star-shaped end-to-end communication and primarily local data flow control would lead to certain problems that can be vividly explained by means of the above-mentioned need for feeding actual consumption data back into the balancing mechanism.

It was already stated in Sect. 14.3 that this balancing mechanism is used to ensure that any supplier procures electricity that exactly equals the aggregated consumption of his own customers for any single 15-min-slot. Obviously, this does not require measurement data that is assigned to individual customers but rather just an aggregated high-resolution consumption value of all customers of a given supplier for any 15 min. This aggregated value must then be known by the supplier (in order to balance overall consumption and procurement) and by the party operating the balancing mechanism (in order to enforce that the supplier actually balances the consumption and procurement assigned to him). Within the chain-formed communication model currently established in Germany, this generation of aggregated high-resolution values is done by the DSO, who then forwards them to the respective receivers. The models pursued for smart meter data communication in the Netherlands and the UK are comparable in this respect.

Under the paradigm of star-shaped end-to-end communication, the only coherent approach for feeding real measurement data into the balancing system would be based on an access profile specifying that the TSO (who operates the balancing mechanism) receives detailed measurement values which are attributed with a supplier-id instead of a customer-specific id. Even in this case, there would be at least a certain risk of the respective data being re-attributed to a certain customer on the basis of consumption patterns – especially when the data arrives in the form of continuous load graphs covering a longer time-frame (i.e. a whole day). In the light of the massive amounts of data that the TSO would receive in this model, some sort of

pre-aggregation at a party not possessing such massive amounts – as present in the established German and the Netherlands' but notably not in the UK's approach – would presumably be preferred from the perspective of data minimization. This would, however, resemble the established concept of chained communication from Sect. 14.5.1 and rather contradict that of star-shaped end-to-end communication between the gateway and the external entity ultimately needing the respective data.

Another example pointing into the same direction is the fact that the still valid regulations given by the German Federal Network Agency assign the tasks of building substitute values in case of missing measurements, of performing a plausibility check on received values and of, where applicable, replacing implausible values by plausible ones to the DSO (see Sect. 14.5.1) in order to prevent significant differences between actual consumption and the consumption values forming the basis for the balancing mechanism. Within the model of star-shaped end-to-end communication, this had to be done by the TSO. It is quite unclear how this should be done without measurement values being attributed to single customers or metering points.

Generally speaking, we will – at least from the current status quo – hardly be able to implement smart metering and smart grids without any personal(izable) data being transmitted to external parties. Furthermore, it can be assumed that at least in some cases, data must be preprocessed in personal(izable) form by one party and then forwarded to another. In any of these cases, the respective data resides beyond the local smart meter gateways and is therefore not covered by the respective, highly formalized technical mechanisms of data flow control based on access-profiles anymore.

For such data residing outside of the customer's smart meter gateway, however, the German legislator merely prescribes that the respective data controllers have to take measures "in accordance with the state of the art in order to ensure data protection and data security […]."[58] Compared to the rather strict requirements for the gateways and their highly formal specification as given with the protection profile and the technical guideline, this requirement is notably vague and unspecific, implying a significant imbalance of requirements. For reasons that can again only be speculated about, the German legislator seems to have focused on the devices that are to be installed at the customers' site alone and to have put much less attention to the systems used by the external parties and the necessary backend processes.

At least the drawbacks of the German approach identified so far should be properly addressed before any kind of potential adoption – be it on a national or even on a European level. In a last step, we will therefore briefly sketch how this could be done and provide suggestions for a concept of technical data protection that actually takes the necessities and givens of the electricity market into account.

[58] See § 21e, 3 EnWG: "Die an der Datenübermittlung beteiligten Stellen haben dem jeweiligen Stand der Technik entsprechende Maßnahmen zur Sicherstellung von Datenschutz und Datensicherheit zu treffen […]."

14.7 Implications for a Possible Adoption

The unquestionably welcome, strong focus on data protection aspects inherent to the German approach to smart meter communication notwithstanding, we can derive at least three implications for any possible adoption of this approach from the above discussion. One with regard to the general procedure of rulemaking in the field of energy data communication, one that refers to the actual subject of regulatory prescriptions for technical data protection with regard to smart metering and finally one that suggests a model for energy data communication which takes the best from the different models presented herein to ensure an adequate level of data protection while still allowing to achieve the goals pursued with the establishment of smart grids under the regulatory givens of the European energy market.

14.7.1 Procedure of Rulemaking

Regarding the general procedure of rulemaking, it should normally go without saying that any approach to modernize an existing, well-functioning and complex system starts with an analysis and thorough examination of the given facts and requirements in order to establish a well-founded understanding of the subject that is to be modernized. With regard to the electricity system, this would in particular have included the well-defined actors and roles of the electricity market, the unbundling regulations governing them and the well-established rules for energy data communication already employed to ensure a well-functioning market. Furthermore, a thorough analysis would have revealed the indispensable need for running a balancing mechanism and for feeding more or less real measurement data into this mechanism in order to actually allow for a better integration of renewables through dynamic, e.g. weather-dependent prices.

None of these facts got significant attention during the initial development of the German approach to data protection within smart metering environments. Instead, the whole approach seems to be largely oriented towards established principles of internet communication, consequently leading to a remarkably strong focus on the local end device, the smart meter gateway. This does, however, lead to miscellaneous drawbacks and uncertainties with regard to the actual implementation of well-established processes. Section 14.6 revealed just some of them.

Any approach for regulating the establishment of smart metering should therefore not repeat this fault but rather start with the established processes of energy data communication that are to be modernized. These processes already address the basic requirements of the electricity market and therefore give reliable advice on the mechanisms and use cases that are to be supported within smart metering environments, too. On the basis of this process knowledge, it should then be discussed how

smart metering can foster the aspired goals, what novel use cases are to be supported within the so-called smart grid and what this implies for the modernization, restructuring or amendment of established processes.[59]

The results of these consideration should then be subject to a thorough analysis of the implications with regard to the customers' data protection rights ("privacy impact assessment – PIA") leading to a well-founded set of aspects actually having to be addressed by techno-legal means of data protection. Only then should it be discussed what modifications should be made to existing processes and communication paradigms and what protective mechanisms are needed to safeguard customers' data protection rights while not preventing the societal goals of energy efficiency and climate protection from being reached. This, and not some intuitively felt need for focusing on the newly introduced devices, should then form the basis for regulatory activities with regard to data protection in smart metering environments.

14.7.2 Subject of Regulatory Prescriptions

This leads us to the second implication regarding the actual subject of regulatory prescriptions for technical data protection. In all likelihood, a thorough analysis as outlined above will reveal indispensable needs for storing, processing and using energy data in personal(izable) form on backend systems operated by external parties and/or needs for such data to be preprocessed by one party before being sent to another. Any comprehensive approach to technical data protection and, in particular, to data-flow- and access-control should thus also appropriately incorporate these backend-systems and establish a consistent level of protection throughout the whole smart metering environment.

Again, the above-mentioned thorough analysis of use-cases and processes will provide valuable guidance about what risks are present at what parts of the overall system and what mechanisms are therefore required to reconcile the "data needs" as implied by the overall goals of smart grids with the customers' inviolable data protection rights. In any case, a regulatory imbalance like the one present in the German approach should be avoided as the customer would otherwise presumably be lulled into a false sense of security by elaborate technical means being locally present to her while the indispensable backend systems put her personal measurement data at serious risk.

[59] The expectable argument that an exhaustive identification of all relevant use cases would be impossible as a matter of principle might again be justified with regard to internet communication. Within the highly regulated energy sector, this is not the case. The relevant market processes are, again as a matter of principle, necessarily well-defined because this is an essential precondition for a competitively functioning, liberalized and unbundled market characterized by natural network monopolies. Use-cases beyond the core energy market, in turn, can very well be generalized to a controlled provision of different data views to external parties.

14.7.3 Outline of an Alternative Model

Instead of ruling out the presumably indispensable need for data being stored, processed and used on backend systems, a sustainable alternative model for technical data protection would therefore accept this need and translate some of the powerful mechanisms now established in Germany from the local smart meter gateway to the systems these backend processes are executed on. Generally speaking, this would put the established model of chained communication with access control being realized in the backend – as pursued in the Netherlands and the UK – to the level of technical data protection that is necessary under a paradigm of smart metering

In particular, this could be done on the basis of trustworthy environments for measurement data being established at the different external parties where – in analogy to the access profiles exerted locally on the gateway in Germany – formally specified sets of rules are applied and cannot be circumvented by the operators of the respective environment themselves. These profiles could then restrict access to the measurement data to those cases unquestionably necessary for operating the liberalized, unbundled market and could also be used to specify operations (anonymizing aggregation, generation of 15-min-values from longer-term ones, replacement of implausible values and substitution of missing ones, etc.) that are to be executed on the data within the trusted environment without releasing the original data themselves.[60] Furthermore, such formalized access rules being applied within a trusted environment at each of the external parties could also serve further principles of data protection like the transparency about actual data uses, data deletion ("the right to be forgotten"), or even external control by data protection authorities.[61]

Such an alternative approach of sending measurement data into a trustworthy environment operated by a dedicated external party and applying the respective access profiles there was also discussed during the German legislation process but strongly opposed by representatives of the federal data protection officer with reference to the principle of data minimization and the supposedly increased risk posed by "centralized data pools".[62] This argument might be appropriate with regard to highly centralized structures like those currently erected in the UK and possibly

[60] The concept of "hippocratic databases" could prove highly valuable here. See Rakesh Agrawal, Jerry Kiernan, Ramakrishnan Srikant, and Yirong Xu, "Hippocratic Databases," Proc. of the 28th VLDB Conference, Hong Kong, China, 2002, pp. 143–154.

[61] See Oliver Raabe et al., "Harmonisierung konträrer Kommunikationsmodelle im Datenschutzkonzept des EnWG." Furthermore, the approach outlined here would also allow to reduce the necessary complexity of the devices being installed at the consumers' sites as compared to the highly complex smart meter gateways now prescribed in Germany – in the light of the massive number of relevant households, this aspect should not be underestimated.

[62] See, for instance, Miriam Pfändler, "Smart Meter und Smart Grid"(paper presented at the Summer Academy of the Independent Center for Data Protection Schleswig Holstein, 2011, p. 5) http://www.datenschutzzentrum.de/sommerakademie/2011/sak2011-ib8-Smart-Meter-und-Smart-Grid-skript.pdf, accessed Nov 28, 2011.

even for those models where data is collected in backend systems by the respective local DSO as it is the case in the Netherlands. The German model, however, allows the customer to assign the role of the metering point operator (MPO) to any (approved) third party at free will. By adopting this practice, it would be possible to establish MPOs as customer-selectable "data trustees" which can be freely chosen on the basis of individual trust, reputation, service quality or even price and to relieve the customer from having to trust a database operator just because of its local responsibility. These data trustees would then operate the databases where measurement data arrives first within a trustworthy environment as outlined above.

May this approach be adopted or not: Any regulatory activity with regard to smart metering and data protection should seriously take the established givens of the electricity market into account and avoid intuitive gut-level decisions, which will in all likelihood prove inappropriate or even reverse the original goal of data protection into its opposite as soon as they are to be transformed into actual implementation.

14.8 Conclusion

The introduction of smart metering is a sine qua non for the establishment of smart grids, which shall serve the overall societal goals of energy efficiency, security of supply and increased integration of renewable energy sources like wind and solar. On the other hand, smart metering allows for a collection of highly detailed, individualized consumption data, thereby raising serious data protection concerns.

In order to appropriately address these concerns, Germany has included extensive regulations with regard to data protection in its recent amendment of energy law. Different from other initiatives across Europe, the resulting "German approach" strongly focuses on the end devices installed at the customers' sites ("smart meter gateways"). We identified four main concepts underlying this German approach, depicted them in relation to the approaches pursued in the Netherlands and the UK and discussed them in the light of the regulatory givens implied by the unbundled and liberalized European energy market.

During this discussion, we identified several drawbacks inherent to the German approach to data protection in smart metering environments. In particular, we showed that the concept of exhaustively defined legitimate purposes does – at least in its current form – actually restrict the customers' right to informational self-determination and that the concept of local preprocessing and tariffing, though unquestionably serving the goal of data minimization, focuses the billing between customer and supplier alone and extensively ignores the need for further billing processes necessary within a liberalized, unbundled market. In a similar vein, the concepts of star-shaped end-to-end communication and solely local data flow control have been shown to not adequately address the actual necessities beyond the local gateway. A functioning and highly dynamic electricity market as envisaged with the development towards "smart grids" necessarily requires potentially personal(izable)

data to be stored, processed and in some cases even forwarded on backend systems operated by external parties. These backend systems should therefore be approached with the same thoroughness that locally installed devices are.

Finally, we derived some implications for any possibly considered adoption of the German approach: The procedure of rulemaking should start with a thorough analysis of existing processes and aspired use-cases and not with a primary focus on the end devices. Regulations should pay attention to the whole system and will in all likelihood also have to cover backend systems and processes. And finally, a possible alternative model could be based on formalized access- and preprocessing-rules being applied on the different market actors' backend systems within trustworthy environments, thereby safeguarding the customers' data protection rights throughout the whole process chain.

Altogether, this boils down to a call for regulations that are made on the basis of a well-founded understanding of the electricity market and it's givens and requirements instead of rather intuitive gut-level beliefs. The overall societal goals of climate protection, security of supply and data protection are too important to be treated with negligence.

References

Agrawal, Rakesh, Jerry Kiernan, Ramakrishnan Srikant, and Yirong Xu. 2002. Hippocratic databases. In *Proceedings of the 28th VLDB conference*, 143–154. Hong Kong, China.

Al Abdulkarim, Laya, and Zofia Lukszo. 2009. Smart metering for the future energy systems in the Netherlands. In *Paper presented at the fourth international conference on critical infrastructures*, Linkoping.

Al Abdulkarim, Laya, and Zofia Lukszo. 2011. Impact of privacy concerns on consumers' acceptance of smart metering in The Netherlands. In *Proceedings of the 2011 IEEE international conference on networking, sensing and control*, 287–292. Delft.

Anderson, Ross, Shailendra Fuloria, and Éireann Leverett. 2011. Data privacy and security for smart meters – response to Ofgem's Consultation. http://www.cl.cam.ac.uk/~rja14/Papers/DECC-sm-final.pdf. Accessed 28 Nov 2011.

Article 29 Data Protection Working Party. Opinion 12/2011 on smart metering. http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp183_en.pdf.

Bauer, Gerald, Karl Stockinger, and Paul Lukowicz. 2009. Recognizing the use-mode of kitchen appliances from their current consumption. In *Smart sensing and context*, Lecture notes in computer science, vol. 5741, 163–176. doi:10.1007/978-3-642-04471-7_13.

BDI – Federation of German Industries. 2010. Internet of energy – ICT for energy markets of the future – The energy industry on the way to the internet age. BDI publication No. 439. http://www.bdi.eu/bdi_english/download_content/ForschungTechnikUndInnovation/BDI_initiative_IoE_us-IdE-Broschure.pdf. Accessed 28 Nov 2011.

BSI – Bundesamt für Sicherheit in der Informationstechnik. 2011. Protection profile for the gateway of a smart metering system. V 1.1.1 final draft. https://www.bsi.bund.de/DE/Themen/SmartMeter/Schutzprofil/schutzprofil_node.html. Accessed 28 Nov 2011.

BSI – Bundesamt für Sicherheit in der Informationstechnik. 2011. TR-03109: Anforderungen an die Interoperabilität der Kommunikationseinheit eines intelligenten Messsystems für Stoff und Energiemengen. V0.2.0draft. https://www.bsi.bund.de/DE/Themen/SmartMeter/TechnRichtlinie/TR_node.html. Accessed 28 Nov 2011.

Bundesrat. Entwurf eines Gesetzes zur Neuregelung energiewirtschaftsrechtlicher Vorschriften. BR-Drucks. 343/11.

Bundestag. Entwurf eines Gesetzes zur Neuregelung energiewirtschaftsrechtlicher Vorschriften. BT-Drucks. 17/6248.

Cavoukian, Ann, Jules Polonetsky, and Christopher Wolf. 2010. SmartPrivacy for the Smart Grid: Embedding privacy into the design of electricity conservation. *Identity in the Information Society* 3: 275–294. doi:10.1007/s12394-010-0046-y.

Davies, Sean. 16, 2010. Internet of energy. *Engineering and Technology* 5: 42–45.

DECC. 2011. Smart metering implementation programme: Response to prospectus consultation – Overview document. http://www.decc.gov.uk/. Accessed 28 Nov 2011.

DECC. 2011. Smart metering implementation programme: Response to prospectus consultation – Supporting document 1 of 5 – data access and privacy. via http://www.decc.gov.uk/. Accessed 28 Nov 2011.

DECC. 2011. Smart metering implementation programme: A call for evidence on data access and privacy. http://www.decc.gov.uk/. Accessed 28 Nov 2011.

Eckert, Claudia. 2011. Sicherheit im smart grid. Alcatel-Lucent-Stiftung. http://www.stiftungaktuell.de/files/sr90_sicherheit_im_energieinformationsnetz_gesamt.pdf. Accessed 28 Nov 2011.

Energie-Nederland. 2011. Energie in Nederland 2011 – Energy in the Netherlands 2011. http://www.energie-nederland.nl/wp-content/uploads/2011/08/Energie-in-Nederland-2011.pdf. Accessed 28 Nov 2011.

European Commission. 2006. European smart grids technology platform – Vision and strategy for Europe's electricity networks of the future. EUR 22040. http://ec.europa.eu/research/energy/pdf/smartgrids_en.pdf. Accessed 28 Nov 2011.

European Commission. 2009. ICT for a low carbon economy – Smart electricity distribution networks. http://ec.europa.eu/information_society/activities/sustainable_growth/docs/sb_publications/pub_smart_edn_web.pdf. Accessed 28 Nov 2011.

European Commission. 2009. Standardisation mandate to CEN, CENELEC and ETSI in the field of measurement instruments for the development of an open architecture for utility meters involving communication protocols enabling interoperability. M/441. http://ec.europa.eu/energy/gas_electricity/smartgrids/doc/2009_03_12_mandate_m441_en.pdf. Accessed 28 Nov 2011.

Greveler, Ulrich, Benjamin Justus, and Dennis Löhr. 2011. Hintergrund und experimentelle Ergebnisse zum Thema 'Smart Meter und Datenschutz'. Technical report – V. 0.6 of Sept. 2011. http://www.its.fh-muenster.de/greveler/pubs/smartmeter_sep11_v06.pdf. Accessed 28 Nov 2011.

Independent Center for Data Protection Schleswig-Holstein. 2011. ULD-Stellungnahme zur Smart-Meter-Regelung im Rahmen der Energiewende. https://www.datenschutzzentrum.de/smartmeter/20110615-smartmeterregelung.pdf. Accessed 28 Nov 2011.

International Energy Agency. 2011. Technology roadmap smart grids. http://www.iea.org/papers/2011/smartgrids_roadmap.pdf. Accessed 28 Nov 2011.

Kamper, Andreas, and Anke Eßer. 2009. Strategies for Decentralised Balancing Power. In *Biologically-Inspired Optimisation Methods*, Studies in Computational Intelligence, vol. 210, ed. Andrew Lewis, Sanaz Mostaghim, and Marcus Randall, 261–289. Berlin: Springer. doi:10.1007/978-3-642-01262-4_10.

Khurana, Himanshu, Mark Hadley, Ning Lu, and Deborah A. Frincke. 2010. Smart-grid security issues. *IEEE Security and Privacy* 8(1): 81–85.

Knyrim, Rainer, and Gerald Trieb. 2011. Smart metering under EU data protection law. *International Data Privacy Law* 1(2): 121–128. doi:10.1093/idpl/ipr004.

Laupichler, Dennis, Stefan Vollmer, Holger Bast, and Matthias Intemann. 2011. Das BSI-Schutzprofil. *Datenschutz und Datensicherheit – DuD* 8: 542–546.

McDaniel, Patrick, and Stephen McLaughlin. 2009. Security and privacy challenges in the smart grid. *IEEE Security and Privacy* 7(3): 75–77.

Müller, Klaus J. 2011. Verordnete Sicherheit – Das Schutzprofil für das Smart Metering Gateway. *Datenschutz und Datensicherheit – DuD* 8: 547–551.

Netbeheer. 2011. Dutch smart meter requirements. V. 4.0 of April 2011. http://www.energiened.nl/_upload/bestellingen/publicaties/284_313185a%20-%20DSMR%20v4.0%20final%20Main.pdf. Accessed 28 Nov 2011.

Pallas, Frank. 2012. Data protection and smart grid communication – The European Perspective. In *Proceedings of the 2012 IEEE PES innovative smart grid technologies conference* doi:10.1109/ISGT.2012.6175695.

Pearson, Ivan L.G. 2011. Smart grid cyber security for Europe. *Energy Policy* 39(9): 5211–5218.

Pfändler, Miriam. 2011. Smart meter und smart grid. Summer Academy of the Independent Center for Data Protection Schleswig Holstein. http://www.datenschutzzentrum.de/sommerakademie/2011/sak2011-ib8-Smart-Meter-und-Smart-Grid-skript.pdf. Accessed 28 Nov 2011.

Quinn, Elias L. 2009. Privacy and the new energy infrastructure. SSRN working paper. http://ssrn.com/abstract=1370731. Accessed 28 Nov 2011.

Raabe, Oliver, Mieke Lorenz, Frank Pallas, and Eva Weis. 2011. Harmonisierung konträrer Kommunikationsmodelle im Datenschutzkonzept des EnWG. In *Computer und Recht*.

Renner, Stephan, Mihaela Albu, Henk van Elburg, Christoph Heinemann, Artur Łazicki, Lauri Penttinen, Francisco Puente, and Hanne Sæle. 2011. European smart metering landscape report. SmartRegions project deliverable 2.1. http://www.smartregions.net/GetItem.asp?item=digistorefile;253415;1522. Accessed 28 Nov 2011.

Task Force Smart Grids – Expert Group 2. 2011. Essential regulatory requirements and recommendations for data handling, data safety, and consumer protection – Recommendation to the European commission. Final draft of June 2011. http://ec.europa.eu/energy/gas_electricity/smartgrids/doc/expert_group2_draft.pdf. Accessed 28 Nov 2011.

Chapter 15
Surveillance as a Service? On the Use of Surveillance Data for Administrative Purposes

Martin Pekárek, Arnold Roosendaal, and Jasper Sluijs

15.1 Introduction

In advance of the annual tax filing due date, in 2011 the Dutch tax authority contacted a number of company car drivers. It had come to the tax authority's attention that they had registered their vehicles for professional use only, which would qualify for a tax exemption when staying under 500 'private' kilometers annually. The 500 km cap may have been exceeded this year, and the agency thus kindly requested the contacted drivers to check their records to make sure their tax return would be filed correctly once due.[1]

This example comes across as a well-intentioned government policy to discourage citizens from erroneous tax filing, fitting in the proactive, service-minded and data-driven 'eGovernment' role that many public authorities aspire to these days. However, the tax authority had reason to believe that the contacted company car drivers had in fact exceeded the 500 km cap, because through Automatic Number Plate Recognition (ANPR) cameras their cars had been spotted at places that suggested extended private use of company cars – say, an IKEA parking lot on a Sunday.

[1] Sameer van Alfen, "Fiscus Bespioneert Leaserijders," *De Telegraaf*, February 11, 2011. See also Jasper Sluijs, "The Dutch Tax Authority and Lease Car Fraud: Institutionalized Intimidation," *TILT blog*, February 28, 2011, http://vortex.uvt.nl/TILTblog/?p=291

M. Pekárek (✉) • A. Roosendaal
Tilburg Institute for Law, Technology, and Society (TILT), Tilburg University,
PO Box 90153, 5000 LE, Tilburg, The Netherlands
e-mail: m.e.pekarek@tilburguniversity.edu; a.p.c.roosendaal@tilburguniversity.edu

J. Sluijs
Tilburg Law and Economics Center (TILEC), Tilburg University,
PO Box 90153, 5000 LE, Tilburg, The Netherlands
e-mail: jasper.sluijs@tilburguniversity.edu

S. Gutwirth et al. (eds.), *European Data Protection: Coming of Age*,
DOI 10.1007/978-94-007-5170-5_15, © Springer Science+Business Media Dordrecht 2013

When factoring into the equation how the Dutch government came to its supposition that some company car drivers may incorrectly file their taxes, this particular policy may become less benign and well-intentioned than it appears at first sight. After all, it turns out that what is presented as a service towards citizens rather seems part of a proactive measure against alleged tax fraud driven by surveillance data. The tax authority collected ANPR data and matched these data to its own administrative data on company car drivers, which yielded a number of hits on people having indicated planning to file for an exemption. The agency thus seemed to presume that the behavior of the contacted driver has been suspect, irrespective of the actual legality of their conduct.

Public authorities play a number of different roles, ranging from the execution of administrative tasks to law enforcement. In the context of law enforcement, distinct competences concerning data collection and processing tend to be strictly defined. However, the above example illustrates that authorities themselves can re-use collected data to be re-employed for administrative tasks under the moniker of a 'service' to citizens.

This mechanism implies that surveillance data, normally employed *ex post* as evidence against suspected offenders, is now used *ex ante* and proactively to 'remind' non-suspects to be law-abiding citizens. This may lead to the assumption that the service is actually an element of an encompassing surveillance and enforcement strategy. Even if this proves not to be the case, the nature and origin of the data make the service problematic because data are used in a context different from the one in which they were originally gathered. Data use in different contexts is not a new phenomenon, but in this case each context is related to a different governmental role, causing this specific type of use to raise questions in terms of foreseeability, legitimacy and accountability of government policy.

The present paper investigates and theorizes this blurring line between enforcement and administrative competences of governments, which is facilitated by data matching techniques. We attribute this recent phenomenon to the advent of behavioral research into public policy. Proactive policymaking ('choice architecture') more closely tailored towards actual human behavior has great advantages. The case of the Dutch tax authority nevertheless seems to suggest that pre-emptive government policy can problematize previously distinct government competences.

In this paper, we highlight a practice that can be described as the proactive use of collected surveillance data, which is enabled by recent developments in technology and data matching practices. We analyze this phenomenon, which we coin as "Surveillance as a Service", and theorize on its underlying mechanisms and its impact on the citizens concerned. We also suggest a number of architectural and procedural measures addressing the blurring role of enforcement and administration through data matching, in which both the objectives of governments and the interests of citizens are better taken into account.

The case of the use of surveillance data to personally address citizens before any criminal offence has occurred is, to our knowledge, hitherto unique. However, it fits within the trend of proactively influencing citizen behavior towards more desirable outcomes, which is part and parcel of modern governance. To date, surveillance techniques and practices had been excluded from these practices, and the current

case of the company car drivers thus represents a major crossroads in this area justifying scrutiny at the earliest opportunity. Moreover, the careful framing of the surveillance practice as a service leads to the assumption that similar procedures may be launched shortly. The analysis offered in this paper may help to instill some appropriate vigilance.

Throughout the discussion, one question may continue to linger in the background with regard to the government-initiated communication in the cases described in this paper: is it a bad thing? Or more specifically: are the rights of the citizens harmed when the authorities implement these practices? There are, *in extremo*, two possible answers to this matter. The first one is affirmative, as some observers would consider the communication unwarranted, and therefore intruding on the private life of the individuals concerned. The opposite reaction is also likely, in which people commend the proactive stance of the government, as it actively helps its citizens to prevent making mistakes. Both answers are possible, and they display two sides of the same coin, as the surveillance of citizens by the authorities always finds itself on the continuum between care and control.[2] We do not pretend to offer a moral judgment on the validity of any of these answers, which is a line of research in current surveillance studies in its own right.[3] The focus of this paper is on analyzing the novel processes at work in the presented cases. The two answers presented above only aim to underscore that some people would not conceive of the described mechanisms and associated communications strategies as being problematic at all.

The remainder of this article is structured as follows. In the next section, three specific cases are presented, each demonstrating a particular government practice subject to discussion in this paper. The section following it further develops the notion of the two faces of government, being the administrative face and the enforcement face. With regard to the latter, Sect. 15.4 explores two types of enforcement (control and investigation) and highlight the differences between the two. Based on these elaborations, the case studies are addressed once again, and analyzed in terms of the government's roles and actions. After that, an alternative approach of dealing with the problems in the case studies is suggested. The paper ends with a summary and some conclusions.

15.2 Case Studies

This section describes three case studies, which serve as a factual backdrop for the developments introduced above.

[2] David Lyon, *Surveillance Studies: An Overview* (Cambridge: Polity Press, 2007).

[3] See e.g., Maria Los, "Looking into the Future: Surveillance, Globalization and the Totalitarian Potential," in *Theorizing Surveillance – the panopticon and beyond*, ed. David Lyon, (Cullompton, UK: Willan Publishing, 2008), 69–94.

15.2.1 Private Use of Company Cars (The Netherlands)

As part of a remuneration package, an employee can be rewarded a company car which typically may also be used for private purposes. In these cases, the benefit of using the car privately is perceived as extra income and is taxed as such. The Dutch tax code, however, states that as long as the private use of the car is lower 500 km/year, the company car is not subject to taxation.[4] To prove that the car has only be used for company purposes, the driver must keep a detailed trip registration in which every single trip is recorded, including trip purpose, starting address, destination address, the distance between the two locations as indicated by the mileage counter, etc.[5]

The driver may file a 'Statement of no private car use',[6] in which the driver states that she does not intend to use the car for private purposes for more than 500 km/year. It is important to realize that even if you have applied for a tax exemption, you are still allowed to drive your car privately as long as you stay under the 500 km cap. The trip registration must be made available to the tax authorities upon request as a control mechanism.

The issue at hand is the following. Based on ANPR data gathered during the fiscal year, the tax authorities proactively contact drivers who have expressed their intention to remain under the 500 km cap. They are reminded of the rules governing the private use of company cars, and are advised to correctly represent the facts in their communications with the tax authorities. These phone calls take place without the tax authorities having had access to the trip registration, and before there is any proof that drivers are actually committing tax fraud. The phone call is triggered by matching the list of drivers who have signed the aforementioned statement, and the vehicles present at locations that indicate private car use.[7]

15.2.2 Data Matching to Evaluate Public Benefits (United Kingdom)

In an effort to eliminate fraud in the public sector, the National Fraud Authority (NFA) – an executive agency of the Home Office of the United Kingdom – launched

[4] Income Taxation Act 1964 (*Wet Op De Loonbelasting 1964*).

[5] The company car drivers thus have to produce surveillance data on their vehicle use, which in itself can be said to put a burden of bureaucratic precision on individual citizens.

[6] In Dutch: "Verklaring geen privégebruik auto". For a downloadable copy of the statement see: http://download.belastingdienst.nl/belastingdienst/docs/aanvraag_lh_verklaring_geen_privegebruik_auto_lh0551z3fol.pdf

[7] The introduction of mass surveillance to verify data supplied by drivers and to then hold them accountable for behavior that is not represented in the disclosed data would only increase the burden mentioned in supra 5. It may lead to self-disciplining of citizens, an effect described in e.g. Michel Foucault, *Discipline and Punish: The Birth of the Prison* (London: Penguin Books, 1991).

a number of pilot studies. In one of these pilots, HM Revenue & Customs (HMRC) and the Department for Work and Pensions (DWP) commissioned private-sector credit reference agencies (CRAs) and data matching companies to verify the circumstances of 20,000 each of benefit and tax credit claimants, in order to identify people falsely claiming to be living alone.[8]

For HMRC, CRAs identified 2,000 high-risk cases which were matched against internal HMRC data, which resulted in letters sent to 750 individuals, requesting them to either submit proof of living alone or cease to apply for this benefit claims. As a result, more than 300 claims were stopped or amended, and more savings are expected once remaining cases are followed up. For DWP, two CRAs identified between 689 and 2,598 Income Support and Jobseeker's Allowance claimants as high risk. After a match with the DWP's internal data, the department expects to save £0.5 m through stopping or amending relevant benefit claims.

The relevant issue in this case is that the government's actions are taken based on information different from data originally supplied to the DWP by the citizens concerned. Instead, other data are used which have been collected and compiled by commercial entities, that do not need to adhere to the same level of accountability and transparency requirements as government institutions with regard to the source and the accuracy of data. Also, since there is no manifest proof of fraud, the government-initiated communication is presented as an administrative service, requesting the citizen to update the information on living circumstances if these, by any chance, may not represent actual arrangements anymore.

15.2.3 ANPR "ring of steel" (United Kingdom)

The town of Royston in Hertfordshire is allegedly the first in Britain that will have ANPR cameras on every approach to town.[9] Seven cameras around Royston will record the number plate of every vehicle that passes them, check the plate against a series of databases and send alerts to police if the vehicle is untaxed, uninsured, suspected of involvement in a crime, or appears on a local or national police "hot-list".[10] Many of the citizen's of Royston react positively or indifferently to the police initiative. However, others are more concerned. A recurring question is why so much information needs to be kept on police records if the sole objective is to catch criminals on the spot.[11]

[8] Cabinet Office and National Fraud Authority, *Eliminating Public Sector Fraud: The Counter Fraud Taskforce Interim Report* (2011), at Annex 2.

[9] Alice Hutton, "Hidden Cameras on All Routes in," *Royston Weekly News*, March 25, 2011.

[10] Angus Batey, "Welcome to Royston … You're under Surveillance," *Guardian*, June 29, 2011.

[11] S.A. Mathieson, "Privacy Groups Take Royston's ANPR Plans to ICO," *Guardian*, June 10, 2011.

This is one of the key elements of the complaint three civil liberties groups have filed with the information commissioner concerning the Royston initiative.[12] The organizations – No CCTV, Privacy International and Big Brother Watch – claim the project is unlawful on a number of accounts. Quoting from a 2010 report of the Hertfordshire Police Authority Scrutiny Committee, car pictures are apparently held for 90 days, and number plate pictures are held for 2 years. These retention periods appear to be excessive when compared to similar international projects (e.g. a comparable Canadian system holds the data for only 72 h).[13] The complaint brings a number of other issues to the fore, such as its failure to meet the requirement of necessity, which should be judged through its proportionality and subsidiarity. At least with regard to proportionality there seem to be problems with the justification of the "ring of steel". Its lawfulness is further challenged by the lack of a specified purpose, and the claimants put forward that generic objectives like "the prevention and detection of crime, public disorder, terrorism and to remove from public roads both unsafe vehicles and unsafe drivers" are far too general to justify the mass collection of data.

For the purposes of this paper, the relevant issue in this case is that enforcement agencies are collecting all license plate information as a matter of routine using blanket surveillance practices, and retain this information for up to 2 years without any justifying cause. Because of the lack of any specified goal for this mass collection of data, it may be put to any use in the months and years to come for aims that by definition are unknown at the time of registration. A database with 2 years of individualized movement data can be mined to discover all sorts of correlations that should be of no interest to a police force if there is no explicit goal whose legitimacy can be challenged in a court of law. The ANPR registration thus puts a liability on the future of everyone whose license plate has been scanned, because developments beyond the control of the individuals concerned may brand them as a potential target for unwarranted police scrutiny in the future, only because their vehicle has crossed the town's limits in the past.

15.3 Proactive Government: A Modern Twist to Classic Roles

This section outlines the phenomenon we coin as 'surveillance as a service,' and theorizes this concept as part of the trend towards more proactive government policy-making that countries like the US, UK and the Netherlands pursue, often based on behavioral insights.

[12] Charles Farrier, Simon Davies, and Daniel Hamilton, "Complaint Letter to the Information Commissioner Concerning Royston ANPR "Ring of Steel"," June 7, 2011.

[13] Information and Privacy Commissioner/Ontario, "Privacy Investigation: The Toronto Police Service's Use of Mobile Licence Plate Recognition Technology to Find Stolen Vehicles," (2003).

Governments in western democracies these days seem receptive towards insights from behavioral (economic) research, which has been popularized by authors like Cass Sunstein and Richard Thaler.[14] Behavioral economics departs from the idea that consumers act as non-rational actors in economic transactions, which is contrary to the basic premises of neo-classical economics.[15] This idea of non-rationality is based on experimental research demonstrating that 'real' people in a lab environment do not rationally maximize welfare as assumed by traditional economic theory.[16]

The findings of behavioral economic research have trickled down into policy circles,[17] leading to innovative ways of 'libertarian paternalistic' policymaking ranging from more efficient ways of registering organ donors via an opt-out mechanism, to incentivizing citizens towards behavior that is more friendly to the environment. Particularly the British government has been very susceptive to behavioral research,[18] where prime minister Cameron even instantiated a 'Behavioral Insights Team' (BIT) as part of the Cabinet Office, whose aim it its to help the UK government develop and apply lessons from behavioral economics and behavioral science to public policy making. In short, it supports government departments in designing policy that better reflects how people really behave, not how they are assumed to behave.[19]

Similar initiatives have been introduced informally in neighboring countries, such as the Netherlands.[20] The British BIT has sparked initiatives in fields as diverse as healthcare, consumer empowerment and energy efficiency.[21] Interestingly, the BIT also endeavors to use behavioral research to fight fraud and other forms of crime and as such collaborates with the also newly instantiated National Fraud Authority (NFA) – also a part of the Cabinet Office. The two groups jointly worked on a successful project where people who had overdue tax debt the year before were

[14] Richard H. Thaler and Cass R. Sunstein, *Nudge: Improving Decisions About Health, Wealth, and Happiness*, 1st ed. (Yale University Press, 2008).

[15] See e.g., Christine Jolls, Cass R. Sunstein and Richard H. Thaler, "A Behavioral Approach to Law and Economics," *Stanford Law Review* 50 (1997): 1471–1550.

[16] For a brief outline of the methodology of behavioral economic research, see: George Loewenstein, "Experimental Economics from the Vantage-Point of Behavioural Economics," *The Economic Journal* 109, February (1999): F25–F34.

[17] Richard H. Thaler and Cass R. Sunstein, "Libertarian Paternalism," *The American Economic Review* 93 (2003): 175–179.

[18] David Wintour, "David Cameron's 'Nudge Unit' Aims to Improve Economic Behaviour," *Guardian*, September 9, 2010.

[19] Gus O'Donnell, "Applying Behavioural Insights," Cabinet Office, accessed November 29, 2011, http://www.cabinetoffice.gov.uk/content/applying-behavioural-insights.

[20] Peter Kooreman and Henriëtte Prast, "What Does Behavioral Economics Mean for Policy? Challenges to Savings and Health Policies in the Netherlands," *De Economist* 158, no. 2 (2010): 101–122.

[21] Cabinet Office Behavioural Insights Team, "Behavioural Insights Team Annual Update 2010–2011," 2011.

contacted informally the next year and were notified of how many people in their region had already filed their taxes on time. This prompted more of these people to file their taxes before the due date.[22]

This successful collaboration between the BIT and NFA was premised on a data matching methodology: a dataset on tax payment of individuals was combined with residential records. Indeed, data matching is a methodology often used to counter fraud, in which formerly unrelated databases are matched to detect fraudulent behavior. Data matching has been embraced enthusiastically by governments,[23] and is increasingly framed by public authorities as well as a way to make relations between citizens and governments more efficient in similar ways as behavioral research is supposed to.[24] It seems that the promise of behavioral research-driven policy fueled by data matching techniques allows for the blending of formerly distinct roles of public authorities. The next section investigates these different governmental roles in more detail.

15.3.1 Two Classic Roles of Government

In daily life, government plays a multitude of roles, which precludes a simple categorization of its roles and responsibilities. For instance, approaches towards definitions of the modern state include, with reference to Weber, Hobbes, and Marx, amongst others, the monopoly of the means of violence, sovereignty, public bureaucracy, and citizenship.[25] However, two faces can be discerned that are readily recognizable. The first one is the government's administrative face. In this role, it takes care of administrative tasks to the benefit of the citizen, such as supplying official documents like passports and driving licenses. It also exercises community functions (e.g. supplying building permits), organizes and upholds certain facilities for the benefit of the people (e.g. the educational system) and takes the lead in large projects that would be beyond the capacities of individual citizens (e.g. large infrastructural works). Although political preferences of the day dictate to what extent the government should play a role in any of these areas, all functions have in essence

[22] Cabinet Office Behavioural Insights Team, "Behavioural Insights Team Annual Update 2010–2011," 2011, p. 17.

[23] Australian Government, "Data-Matching Program (Assistance and Tax) Act 1990," *C2006C00591*, 1990.

[24] "Ultimately, improving data matching will help us to better measure the effectiveness of multiple programs, and more efficiently target resources to achieve goals like promoting more work and earnings, reducing poverty, and ending dependence on government benefits. These are goals that we should all agree on.", U.S. House of Representatives, Committee on Ways and Means, *Human Resources Subcommittee Hearing on the Use of Data Matching to Improve Customer Service, Program Integrity, and Taxpayer Savings*, March 11, 2011.

[25] C. Pierson, *The Modern State*. (London: Routledge, 2004), pp. 4–26.

been delegated to the government for reasons of fairness, efficiency, and effectiveness. This is the area in which the authorities are perceived as delivering 'services' to the citizens.

The second face of government is its enforcement face. This is the area in which it upholds the law, and executes associated tasks like crime prevention and criminal prosecution. For these purposes, the government is bestowed with investigative powers that are strictly regulated and may only be exercised if certain conditions are met. Also, only specified actors within the government domain, of which the police are a prime example, may use these powers. The distinction between the administrative face and the enforcement face of government is not clear-cut in every area. Take for instance the tax domain. Many of the tasks belong to the administrative realm, such as the yearly processing of income tax filings and the collection of the amounts due. However, tax authorities are granted enforcement powers as well, which may be exercised in order to collect assets from tax subjects who are unwilling to pay, or to commence investigative actions when tax fraud is suspected.

In practice, the two faces can be distinguished in most Western jurisdictions, even though the exact definition of the purpose of the state and the scope of this purpose shows variations. This is due to differences in the development process of the state and its functions, in particular between civil law jurisdictions as can be found on the European continent and the Common Law tradition of the United Kingdom. The UK is a state, but not a nation, and its evolvement has taken place along the lines of rather uncoordinated events that, step by step, developed the legal relations between the state and the citizens, as well as the distribution of powers.[26]

At a more fundamental level, the two faces can be related to the classical (democratic) constitutional state and the social constitutional state. In the classical constitutional state, the role of the government was mainly related to the protection of constitutional rights based on fundamental rights. In order to offer this protection, certain acts, such as murder, violence, and discrimination, were legally prohibited, and the state was empowered with enforcement capacities to uphold the law. This role of the state can also be referred to as *Ordnungspolitik* or the aggrandizement of power of the *Machtstaat*.[27] This role forms the basis of the investigative powers related to the enforcement face.[28] The social constitutional state is offering more 'social' protection, such as health care and education, and employment facilities. This is more related to the administrative face, including regulating health care standards and providing documents that allow people to work or receive education.[29] Other indications for this role are the *soziale Gestaltungspolitik* or the 'educative state' as the basis of social morality.[30]

---

[26] J. Alder, *Constitutional and Administrative Law*. (Hampshire: Palgrave Macmillan, 2005), pp. 94–95.

[27] K.H.F. Dyson, *The State Tradition in Western Europe; A Study of an Idea and Institution*. (Oxford: Martin Robertson, 1980), p. 223.

[28] M.C. Burkens et al., *Beginselen Van De Democratische Rechtsstaat*. 5th ed. (Deventer: W.E.J. Tjeenk Willink, 2001), p. 18.

[29] M.C. Burkens et al., *Beginselen Van De Democratische Rechtsstaat*. 5th ed. (Deventer: W.E.J. Tjeenk Willink, 2001), p. 26.

[30] K.H.F. Dyson, *The State Tradition in Western Europe; A Study of an Idea and Institution*. (Oxford: Martin Robertson, 1980), p. 223.

Tensions ensue when, in the interaction with citizens, government presents its administrative face using information, which it may only have gathered in its enforcement role. The first case supplied in the previous section is a good example of this practice. ANPR data, the collection of which is sanctioned by the government's enforcement powers, are used to directly address people through channels that – until that day – have been used as the administrative face of government. The example illustrates a tendency amongst policymakers in which administrative and law enforcement tasks blend into each other. However, it should be borne in mind that administrative duties and law enforcement are based on distinct competences that through policies such as the one described above may become mingled. This raises questions of foreseeability, legitimacy and accountability of government policy. Proactive government policy may be more efficient; it can also be intrusive and premised on an authority that is legally suspect.

15.4 Control vs. Investigation

It is useful to distinguish between two typical powers that may be invoked by authorities to uphold the law, 'control' and 'investigation'.[31] Actually, these two powers have their own distinctive competences attributed to authorities. First, the power of 'control' allows the authorities to check whether the general public adheres to the rules as codified in law. One example are speed traps: by measuring the velocity of all passing vehicles at a designated spot, it is possible to probe whether the drivers adhere to the limits set out in the law. The characteristics of 'control' are twofold. First, it is not required that an unlawful act has been committed before the control mechanism is employed. By definition, it is only by using the control mechanism that unlawful acts can be detected, and control measures therefore have a preventative nature.[32] Thus, setting up a speed trap does not require the evidence that people have been speeding at that location. A second important characteristic is that control is indiscriminate (i.e. not personalized). Any subject that satisfies the definitions in the law (e.g., drivers of motor vehicles) is checked when the control mechanism is put in place, without any knowledge (nor interest, for that matter) about the identity of the driver. It is only after an offense has been established that the identity of the driver is required, because an essential element of enforcing this particular law is to fine the responsible driver for his failure to observe the set speed limits. In cases where rights and freedoms of citizens may be affected, the exercise of control measures has to be legitimized

[31] G.J.M. Corstens, *Het Nederlands Strafprocesrecht*, 3rd ed. (Deventer: Gouda Quint, 1999), p. 21.

[32] G.P.A. Aler, *De Politiebevoegdheid Bij Opsporing En Controle* (Zwolle: W.E.J. Tjeenk Willink, 1982), p. 4 and 30.

by legal provisions. Moreover, there may be no conflict with non-codified law nor with general legal principles.[33]

The second power is the power of 'investigation'. In such a case, there is always an immediate cause to start an investigation. One reason may be that it is obvious that a crime has been committed (e.g., a murder victim is found), or if there is a strong suspicion that a criminal act has occurred (e.g., the data provided on a tax return give the impression of fraudulent behavior). When the criminal investigation is started, there is often already someone suspected (e.g. the filer of the tax return), which contrasts with the concept of 'control' introduced above. Even when there is no suspect yet, for instance in a murder case without any witnesses, the investigation is still aimed at discovering the identity of the individual responsible for the crime. In other words, investigations are conducted only after sufficient justification is established in the form of substantial evidence or specific suspect behavior. Investigative powers are therefore applied in an *ex post* fashion. The use of investigative competences requires a concrete suspicion of a criminal act.[34] This act has to be punishable as provided by a specific legal provision, which implies that as long as there is no punishable act, the exercise of investigative powers is not allowed.[35]

Tensions arise when control measures take the form of an investigation. This is the case in the first case supplied in Sect. 15.2. There are rules about the conditions under which a taxpayer may claim exemption to having to pay additional taxes on the use of a company car. Ordinarily, these rules would be upheld through the process of control: after the tax return has been filed, a check would be performed on all company car drivers to see whether they adhere to the rules. Only after a suspicion arises that some of these claimants have not played by the book, an investigation may be conducted into the details of the individual tax returns of these drivers. Thus, the move from the control regime to the investigation regime (and the associated move from a general regime to an individualized regime) is only made after establishing suspicious behavior. This is, once again, an example of *ex post* investigation.

In this case, the individuals are subject to an investigative approach before they have filed their tax return, i.e. before there is any data provided by the tax subjects themselves, which might garner an interest by the investigating authorities. Instead, the data leading to an individual investigation are collected using a 'control' approach, in which first all vehicles present at a certain location and time are registered using ANPR with the specific purpose to enforce taxation laws.[36] Then, a

[33] G.J.M. Corstens, *Het Nederlands Strafprocesrecht*, 3rd ed. (Deventer: Gouda Quint, 1999), p. 22.

[34] G.P.A. Aler, *De Politiebevoegdheid Bij Opsporing En Controle* (Zwolle: W.E.J. Tjeenk Willink, 1982), p. 29.

[35] G.J.M. Corstens, *Het Nederlands Strafprocesrecht*, 3rd ed. (Deventer: Gouda Quint, 1999), p. 15.

[36] In a similar fashion, speed cameras are used as a tool to enforce speed limits and to catch speeding incidents, Both approaches qualify as control measures, because all cars within reach of the cameras are recorded *for a specific purpose that has been defined in advance.*

data match is conducted, in which all company car drivers who have indicated that they are planning to stay within the 500 km exemption are highlighted. Only this specific subset is addressed in a one-to-one 'reminder' by the tax authorities. It is important to remember that the presence at that time and location in itself is not illegal, as the occasional trip to the IKEA may well fall within the limits of the 500 'private' km cap. Only if these drivers would claim on their tax returns not to have exceeded the 500 km cap and proof would show this to be a misrepresentation of facts, there would be a good case for an individual investigation. Instead of the *ex post* investigation which is customary in case of criminal investigations, the *ex ante* investigation which befalls the company car drivers concerned represents a radical new notion of the authorities' enforcement role, as will be further analyzed in the next section.

15.5 Analysis

In all three cases of Sect. 15.2, surveillance elements are present, but the means of data collection and the presentation of data analysis findings to the individuals differ.

In the case of the ANPR "ring of steel" around the town of Royston, the data are collected on account of the enforcement powers of the authorities. In fact, the Royston case is a demonstration of a 'control' approach, which moves to investigation after a match with any of the connected databases occurs. This approach is becoming increasingly prevalent, and is a demonstration of the electronic execution of traditional enforcement powers. However, in cases where there is no match, the collected ANPR data remain on file with the authorities for up to 2 years, which calls into question the proportionality and subsidiarity of the measure: one can seriously wonder whether the demonstrated blanket surveillance and massive data collection meet these criteria. The consequence of this long-term data retention of detailed ANPR data is that the potential for an individual investigation keeps looming, and may be triggered by circumstances that are unknown at the time of registration. If such an investigation would befall any of the individuals whose vehicle is associated with any misdemeanor in the future, the authorities are likely to exercise all enforcement powers available to them.

In contrast to the above case, the example of data matching to prevent fraud in the UK does not use surveillance data recorded on account of an enforcement power. Instead, commercially available information is acquired and combined with information on file with the authorities. In principle, any output that would result in a high suspicion of benefit fraud would lend itself to the start of an investigation aimed at specific individuals, but in this case authorities decided to ask benefits recipients whether their files still reflected the actual situation. The advantages of this approach are obvious: one well-written reminder has an immediate and sizable effect, and does away with the necessity of commencing individual investigations that may take much time and effort (and funds) to complete in accordance with the strictly defined

legal provisions. Thus, some of the data used are obtained from non-governmental sources, and the people who are suspect are approached individually. As opposed to the Royston case, the consequence of this strategy is that the authorities cannot use their enforcement face, since no official investigation has been started: the communication must necessarily be drafted as an administrative matter.

A similar situation exists in the case of the company car drivers, in which no crime has been committed before the drivers file a fraudulent tax return, which is why the authorities cannot rely on their enforcement face. Still, they want to stimulate taxpayers to represent the facts concerning the private use of their cars correctly, which explains why they have to revert to their administrative face and present their findings as a service to the individual company car drivers, in spite of the fact that relevant data have been gathered through enforcement competences. Surveillance as a Service sees the light, and the practice may be considered as intimidating by many company car drivers, particularly because the individualized approach normally reserved for criminal investigations is now applied in a situation which would only justify a regular 'control' procedure.

The last two cases are also applications of behavioral economics in policy circles, a trend that was highlighted in Sect. 15.3. The mere suggestion by the authorities of their willingness to apply their enforcement powers intends to nudge individuals into desired behavior, thus rendering a personalized investigative route superfluous. The case of the company cars is in this respect all the more remarkable, since this is an example in which surveillance data gathered by the authorities employing enforcement capabilities are actively used to steer citizen's behavior to align with governmental objectives without reverting to investigative action.

The question remains why the phenomenon described in the three case studies triggers feelings of unease amongst many people. More importantly, the developments discussed here are symptomatic of the use of investigative powers in a growing number of areas, spurred by the possibilities offered by new technologies. This potentially has serious consequences for the organization of society, especially concerning the power balance between the citizens and the state. In an attempt to identify certain thresholds that might be crossed in such processes we will further analyze the first case study in a step-by-step fashion.

As a starting point, it should be acknowledged that the type of fraud possible with the private use of company cars can only be combated when information is collected on the actual use of the vehicle in the year previous to filing date of the tax return. So, if someone drives a company car throughout 2012, the tax return is due only by April 1, 2013. If the authorities want to call the correctness of the tax filing into question, they would logically need to have information on the actual use in 2012 at their disposal. Otherwise, they would not be able to have any proof in case of a prosecution. The use of ANPR to collect information for such purposes is thus understandable, as it is merely deployed as a technique to collect relevant data for a specific aim at a particular location for a restricted period of time. Moreover, a proper implementation of ANPR technology would allow for immediate deletion of non-relevant data, thus staying within the confines of the purpose of the data collection (i.e., control against illegitimate private use).

It is also a logical step to match the information collected through ANPR with the identity of the individual company car driver when an actual act has occurred which would justify such a data matching procedure. This is the straightforward method of producing incriminating evidence against suspected tax evaders. So far, few people would object to this practice. However, should the data still be matched when an actual justification for that step is lacking? One may argue that this is not a problem as long as this information is kept within the confines of the tax authorities. Nevertheless, the mere act of data matching creates a new category of tax subjects, namely a group of people who have driven their car privately but who have stayed within the limits of the law. It may be claimed that, exactly because the individuals remain within the limits of the law, they do not merit special attention. Without a good reason, this category should not be created to start with, as flagging is vulnerable to function creep.[37] By creating these types of unwarranted categories, certain questionable scenarios become possible. Imagine what would happen if you were to fall into this category for a few years in a row: some tax inspector might consider you to be a high profile target for a closer inspection, although you have never strayed outside the law.

The final step is that the individual company car driver is confronted with the data match before she has committed the act of falsely representing facts on a tax return. There are serious questions to be posed concerning this proactive approach, because there has never been an act[38] to merit such individual attention by the tax authorities. The fact that a probabilistic approach to some future decision is taken ("People who go to the IKEA on Sundays with their company car are likely to commit fraud in their tax return."), in fact implies that the entire concept of the "presumption of innocence" is dropped. At least, you are apparently a little less innocent if you belong to a group of people who, statistically spoken, are more likely to commit fraud.[39]

Overall, one specific effect is that the innocence of people is not used as a starting point anymore. Under Dutch law, the definition[40] of a criminal offense is a fact (which can be performing or neglecting an act) that is unlawful and attributable to blame. In

[37] See e.g., Christine Bellamy, "Alive and Well? The 'Surveillance Society' and the Coalition," *Public Policy and Administration* 26, no. 1 (2011): 149–55, and Wetenschappelijke Raad voor het Regeringsbeleid. *iOverheid* (Amsterdam: Amsterdam University Press, 2011).

[38] In Dutch: handeling.

[39] Statistical inference using data collected through surveillance may result in social sorting, discrimination and accumulated disadvantage. See e.g., Oscar H. Gandy, "Quixotics unite! Engaging the pragmatists on rational discrimination," in *Theorizing Surveillance - the panopticon and beyond*, ed. David Lyon, (Cullompton, UK: Willan Publishing, 2008), 318–336. In this particular case, the subgroup of people who visit IKEA on Sundays is also more intensively scrutinized as a result of the classification process described. The societal effects are however less prevalent, because the subgroup is less susceptible to future discrimination.

[40] In Dutch: "Voor een strafbaar feit moet sprake zijn van een feit, dat in strijd is met het recht en waarvan de bedrijver een verwijt gemaakt kan worden (dus waaraan deze schuld heeft)", J. Remmelink, *Inleiding Tot De Studie Van Het Nederlandse Strafrecht*, 14th ed. (Arnhem: Gouda Quint B.V., 1995), p. 126.

the cases described in this paper, the fact mentioned in the definition is lacking. Therefore, there is no rightful justification for the use of investigative powers. More and more applications of data matching are becoming a reality thanks to the increasingly more powerful possibilities afforded by modern technologies to support massive data collection against low costs. These rapid technological developments may unwittingly underexpose the requirement of a fact for the law to apply.

15.6 Process Modification

The analysis has shown in detail what consecutive steps are taken in cases that present surveillance as a service. Even without taking a moral stance on the acceptability of the approach, one can safely assume it yields positive effects in terms of increased tax income and a lesser need to launch costly investigations. One wonders whether the same benefits might materialize using the same (types of) technology, but without the associated surveillance aspects. In our opinion, this should be feasible by adapting the data collection and matching process in line with the suggestions provided below for the company car case. The suggestions are based on basic principles of data protection as laid down in Directive 95/46/EC.[41]

In order to examine whether people truthfully represent the actual circumstances during the time period subject to taxation, it is necessary to collect information during that period. Only by confronting the claims of the tax subjects with the evidence gathered by the tax authorities throughout the fiscal year, irregularities may become apparent, which may lead to further investigations. In case of the company cars, it is therefore acceptable that ANPR data are collected of cars at potentially suspect locations, such as border crossings during holiday weekends.

The choice of so-called suspect locations is critical, as it must balance the requirement of collecting enough relevant data to be used as a basis for effective fraud investigations with the need to prevent disproportionate surveillance. This would justify the focus on times and places where one would not expect business use of company cars (e.g., the IKEA parking lot on a Sunday). A potential problem is constituted by false positives caused by the systemic consequences of the data collection setup (e.g., an IKEA employee with a company car working on Sundays, who might find herself to be the subject of a closer investigation). Such effects are inevitable, but may be perceived as an acceptable downside of the control system. It is key to understand these systemic effects in advance and treat them with due caution, such as by basing all subsequent investigative steps on the presupposition that the subject is indeed a false positive. If this is done prudently, the impact on the lives of the people finding themselves in these suspect locations may be minimized.

[41] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281, 23.11.1995, pp. 31–50.

In the proposed modified procedure the collected data – only existing of a license plate number associated with a location and a time stamp – are not processed any further, but are stored at a secure location until the moment the tax filings are received (i.e. in the year following the year in which we want to establish the potential private use of company cars). At that time, it is possible to match the number plates of the taxpayers who claim to stay below the 500 km threshold with the number plates of vehicles that have been spotted at unusual locations. Only when the same license plate is encountered in both files, there is a justified reason to start an investigation. This is the moment in which the 'hits' may be enriched with personal data of the drivers, which may subsequently be contacted as part of an investigation. All other ANPR data may be destroyed after the initial data match, as these would not benefit any further investigative purposes.

The proposed alternative process effectively protects the interests of all people who are not concerned, and it complies better with certain principles set out in the national implementations of the European Data Protection Directive.[42] For instance, if the essential step of enriching the set of license plates with personal information of the vehicle drivers is performed after the data match between the ANPR data with the tax returns, the principle of data minimization as laid down in article 6(3) of the Directive[43] is better respected. Another example is the concept of purpose specification as expressed in Art. 6(1) (a) of the Data Protection Directive, which requires that "[…] personal data must be collected for a specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes." Once again, the enrichment of the ANPR data with additional personal information after the data match would better respect this principle[44] than the current practice, because the particular processing act would be specifically linked to the express purpose of combating tax evasion. In short, both processing steps should only be taken if a specific purpose is present. The first step is building a data set for future reference, and the second step is enhancement of the data set with additional personal information of individuals whose deeds actually qualify them as a suspect (i.e. after the filing of their tax return).

The net result of data protection in this alternative model is that citizens who are not suspect are not confronted with individual 'warnings', thus protecting them from undue collection and processing of data. Moreover, clear guidelines

[42] Directive 95/46/EC has been implemented in the national legislation of each EU member state (e.g., the Wbp in the Netherlands and the DPA in the United Kingdom).

[43] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281, 23.11.1995, pp. 31–50.

[44] We refer to the Personal Data Protection Act as the legal framework against which the processing of personal data should be assessed. Considering the nature of the cases, and the involvement of actors with investigative powers, specific laws related to these actors are relevant as well. These laws contain comparable data protection principles. The point is that – no matter which legal regime is applicable – the suggested alternative process respects these principles better than the current practice does.

and associated communication on the enforcement practices employed would also make such systems transparent and amenable to public (legal) scrutiny. An important consequence of our proposed model is that more ANPR data need to be retained for a longer period, which may seem counter-intuitive from a data protection perspective. However, the focus is not on the storage of the data but on their eventual use. In fact, we are encouraging authorities to exercise restraint in the further processing of data through data matching.

The proposed alternative process eliminates the individualized investigation preceding the actual act of filing a tax return, and would thus remove the surveillance character of the tax authorities' behavior. However, the authorities might still be able to effectively nudge taxpayers into filing a correct tax return. By generally announcing that the information supplied by company car drivers will be the subject of intensive scrutiny in a certain year, the prospective taxpayers may be forewarned and adjust their tax filing behavior accordingly. Such a warning may even be communicated to company car drivers only, thus targeting a specific group of taxpayers. The nudging effect of addressing the entire population of company car drivers as a group at the moment of filing the tax return instead of as individuals at a moment months prior to the filing may indeed be somewhat lower. However, it has as a distinct advantage that it does not rely on the disciplining effects of surveillance as a service.

15.7 Conclusion

This paper employed three cases to illustrate a shift in the relationship between the government and its citizens when it comes to the use of surveillance data for law enforcement purposes. The case of the ANPR cameras surrounding the town of Royston was a demonstration of surveillance data to be used for individual investigation after a violation of the law has been established. Because of its *ex post* character, the authorities can thus use their enforcement face during prosecution. In the case of data matching using information from commercial credit rating agencies to elicit potential fraudsters, the people targeted were not prosecuted but simply asked whether the information held on them was still accurate. As individual investigations are not under discussion yet, the authorities cannot rely on enforcement measures, but have to present their actions as administrative matters. In the last case of the company car drivers there is again no individual prosecution, but this time the authorities rely on surveillance data obtained through enforcement powers as a basis for addressing certain citizens. This particular construct was dubbed "Surveillance as a service", because the authorities themselves frame their actions as proactively providing services aimed at making life easier for citizens by helping them to prevent any unfortunate mistakes.

All cases use data matching as a starting point, but only the first aims to use the newly created information to start individual investigations after a violation of the law has been established. The last two cases demonstrate how the authorities aim to

guide citizens into desired behavior *before* any proof of a criminal offense exists. Merely raising the awareness of the potential availability of incriminating information should be sufficient to reach certain government objectives, nudging citizens to do the right thing without having to resort to costly individual investigations.

The use of surveillance data to influence people before any factual proof exists may be considered by some as intrusive, as it removes essential elements of the expected safeguards against government interference with citizens' private lives. By outlining a modified process with regard to the last case, we demonstrated that similar policy objectives may be attained without resorting to the potentially intimidating use of enforcement data. Although the nudging effect may be somewhat lower, the transgressive use of surveillance data to exert influence on an individualized level without proof of an unlawful act is thus constrained.

Acknowledgement The authors greatly acknowledge the anonymous reviewers for their valuable comments on draft versions of this paper.

References

Alder, J. 2005. *Constitutional and administrative law*. Hampshire: Palgrave Macmillan.

Aler, G.P.A. 1982. *De politiebevoegdheid bij opsporing en controle*. Zwolle: W.E.J. Tjeenk Willink.

Alfen, Sameer van. 2011. Fiscus Bespioneert Leaserijders. *De Telegraaf*, February 11

Australian Government. 1990. Data-matching program (Assistance and Tax) Act 1990. In *C2006C00591*.

Batey, Angus. 2011. Welcome to Royston … You're under surveillance. *Guardian*, June 29.

Bellamy, Christine. 2011. Alive and well? The 'surveillance society' and the coalition. *Public Policy and Administration* 26(1): 149–55.

Burkens, M.C., H.R.B.M. Kummeling, B.P. Vermeulen, and R.J.G.M. Widdershoven. 2001. *Beginselen van de democratische rechtsstaat*, 5th ed. Deventer: W.E.J. Tjeenk Willink.

Cabinet Office Behavioural Insights Team. 2011. *Behavioural insights team annual update 2010–2011*.

Corstens, G.J.M. 1999. *Het Nederlands strafprocesrecht*, 3rd ed. Deventer: Gouda Quint.

Dyson, K.H.F. 1980. *The state tradition in western Europe; a study of an idea and institution*. Oxford: Martin Robertson.

European Commission. 1995. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. *Official Journal L* 281: 31–50.

Farrier, Charles, Simon Davies, and Daniel Hamilton. 2011. *Complaint letter to the Information Commissioner Concerning Royston Anpr "Ring of Steel"*, June 7.

Hutton, Alice. 2011. Hidden cameras on all routes. *Royston Weekly News,*.March 25.

Income Taxation Act 1964 (Wet Op De Loonbelasting 1964).

Information and Privacy Commissioner/Ontario. 2003. *Privacy investigation: The Toronto Police Service's use of mobile licence plate recognition technology to find stolen vehicles*.

Jolls, Christine, Cass R. Sunstein, and Richard H. Thaler. 1997. A behavioral approach to law and economics. *Stanford Law Review* 50: 1471–1550.

Kooreman, Peter, and Henriëtte Prast. 2010. What does behavioral economics mean for policy? Challenges to savings and health policies in the Netherlands. *De Economist* 158(2): 101–122.

Loewenstein, George. 1999. Experimental economics from the vantage-point of behavioural economics. *The Economic Journal* 109(February): F25–F34.

Los, Maria. 2008. Looking into the future: Surveillance, globalization and the totalitarian potential. In *Theorizing surveillance – The panopticon and beyond*, ed. David Lyon, 69–94. Cullompton: Willan Publishing.

Lyon, David. 2007. *Surveillance studies: An overview*. Cambridge: Polity Press.

Mathieson, S.A. 2011. Privacy groups take Royston's ANPR plans to ICO. *Guardian,* June 10.

O'Donnell, Gus. Applying behavioural insights. Cabinet Office, http://www.cabinetoffice.gov.uk/content/applying-behavioural-insights

Pierson, C. 2004. *The modern state*. London: Routledge.

Remmelink, J. 1995. *Inleiding tot de studie van het Nederlandse strafrecht*, 14th ed. Arnhem: Gouda Quint B.V.

Sluijs, Jasper. The Dutch tax authority and lease car fraud: Institutionalized intimidation. http://vortex.uvt.nl/TILTblog/?p=291

Thaler, Richard H., and Cass R. Sunstein. 2003. Libertarian paternalism. *The American Economic Review* 93: 175–79.

Thaler, Richard H., and Case R. Sunstein. 2008. *Nudge: Improving decisions about health, wealth, and happiness*, 1st ed. New Haven: Yale University Press.

U.S. House of Representatives, Committee on Ways and Means. 2011. Human resources subcommittee hearing on the use of data matching to improve customer service, program integrity, and taxpayer savings, March 11.

Wetenschappelijke Raad voor het Regeringsbeleid. 2011. *iOverheid*. Amsterdam: Amsterdam University Press.

Wintour, David. 2010. David Cameron's 'Nudge Unit' aims to improve economic behaviour. *Guardian,* September 9.

Chapter 16
Profiling – the Council of Europe's Contribution*

Jörg Polakiewicz†

16.1 Why Is the Council of Europe Dealing with Profiling?

Privacy and data protection have always been core values of the Council of Europe. The Committee of Ministers is expected to adopt shortly a Council of Europe Internet governance strategy, which contains a whole chapter on advancing privacy and data protection. Our activities are centred around:

- the European Convention on Human Rights ("ECHR"), thanks to which the right to privacy is a directly enforceable fundamental right since 1953, nowadays for 800 million Europeans, and
- the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (convention 108[1]) and its additional protocol.

The protection of personal data falls within the scope of private life as protected by Article 8 of the ECHR. On 23 November 2010, the Committee of Ministers

*Privacy Platform Meeting COMPUTERS READING OUR MINDS? The benefits and risks of profiling Brussels, 25 January 2012. Profiling – The Council of Europe's contribution

†Head of Human Rights Policy and Development Department, Directorate General Human Rights and Rule of Law, Council of Europe, and Professor at the *Europainstitut* of the University of Saarbrücken. This article was written in a strictly personal capacity and does not necessarily reflect the official position of the Council of Europe.

[1] "Council of Europe Convention 108", accessed 27 February 2012, http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=108&CM=8&DF=19/01/2012&CL=ENG.

J. Polakiewicz (✉)
Directorate General Human Rights & Rule of Law (DGI), Council of Europe,
Agora Building Office C6,07V, 67075 Strasbourg Cedex, France
e-mail: jorg.polakiewicz@coe.int

S. Gutwirth et al. (eds.), *European Data Protection: Coming of Age*,
DOI 10.1007/978-94-007-5170-5_16, © Springer Science+Business Media Dordrecht 2013

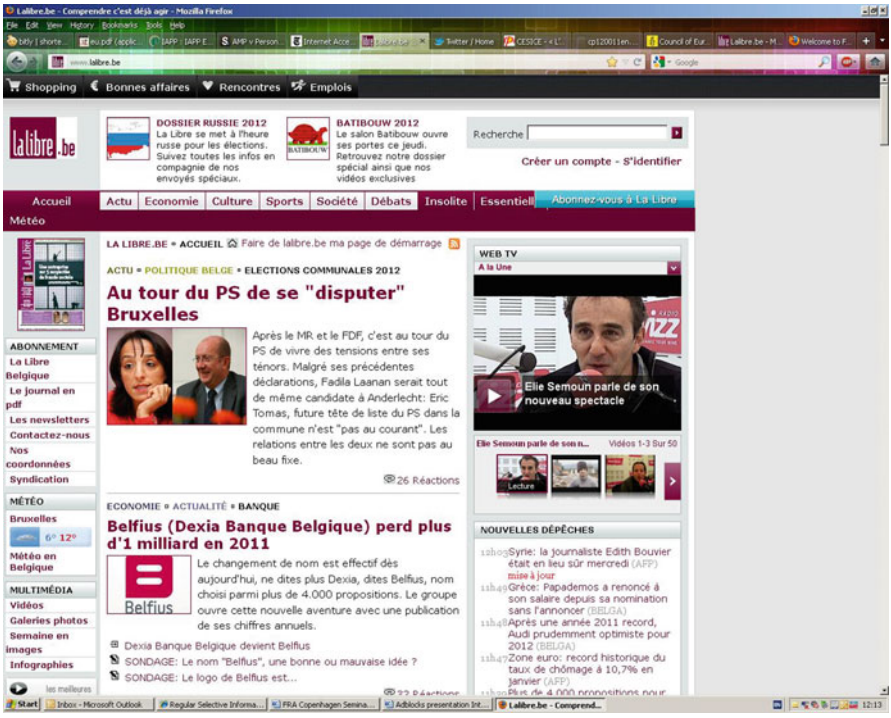
adopted Recommendation CM/Rec(2010)13[2] on the protection of individuals with regard to automatic processing of personal data in the context of profiling, the first internationally agreed standard dealing specifically with this topic. This recommendation is the most recent of several so-called sectoral recommendations adopted on the basis of Convention 108. Their aim is to ensure that the collection and processing of data in a given sector (e.g. banking, insurance, health, police) or carried out using a particular technique or technology (e.g. smart cards or in our case profiling) are carried out in accordance with the rules and principles of Convention 108.

Before explaining the objectives, scope and content of this recommendation, I would like to give an example of the risks involved in profiling.

16.1.1 Demonstration: The Challenges for Privacy Resulting from the Use of Transclusive Hyperlinks

Profiling techniques are used in particular in online advertising, where individual browsing habits are often tracked and collected without notice and permis-

Slide 1

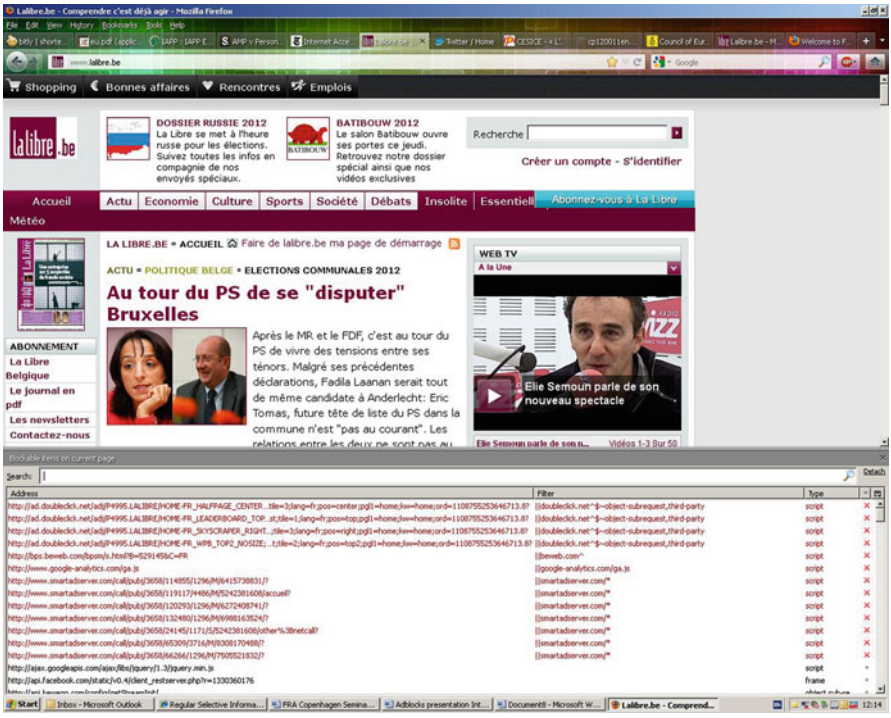


[2] "Council of Europe Recommendation CM/Rec(2010)13", accessed 27 February 2012, https://wcd.coe.int/ViewDoc.jsp?id=1710949&Site=CM. See Jean-Philippe Walter,"Le profilage des

sion. Let us take the example of a user who consults a popular newspaper on-line.

When the web page is requested, a transclusive hyperlink is added, ordering the browser to download content from external servers. What actually happens can be made visible through 'Adblock Plus'. This slide shows the Adblocks hyperlinks.

Slide 2

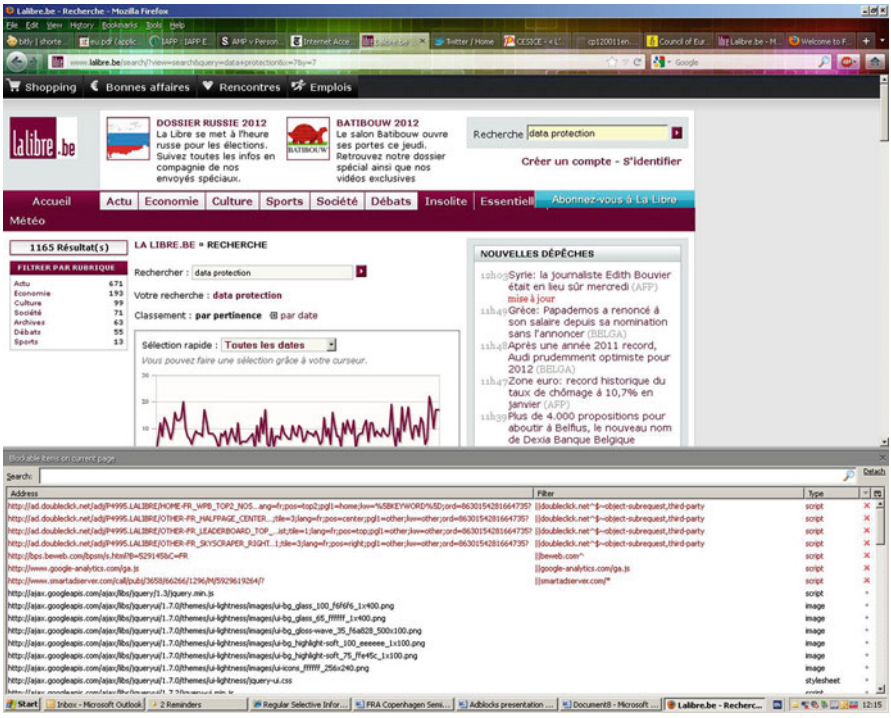


The average user has no means to oppose these connexions. They remain invisible. The browser will communicate to third parties, such as advertising companies or Google analytics, the exact URL reference of the article the user is reading. This transmission of information may also include keywords typed in search engines or interventions made in discussion forums (see Slide 3).

When the same advertiser is present on several websites which are systematically using a permanent unique identifying cookie, it collects on a daily basis the click stream of the majority of users providing a rather detailed view of their use of the Internet. The following slide shows a popular site with Double-Click present in the Adblock window.

individus à l'heure du cyberespace : un défi pour le respect du droit à la protection des données", in: Datenverknüpfung: Problematik und rechtlicher Rahmen, Zürich: Schulthess, 2011, 87–114.

Slide 3



16.2 The Recommendation's Objectives

New information and communication technologies (ICT) facilitate the observation and storage of most day-to-day human activities more easily, rapidly and invisibly than ever before, such as buying and selling, searches, reading newspapers, sending and receiving emails. The recommendation underlines that the increasing use of profiling techniques poses a threat to private life, understood as an individual's capacity for self-determination.

Two risks are worth highlighting: (1) the inevitable uncertainty as to the accuracy of profiles and (2) the conclusions drawn from them and data decontextualisation.

Firstly, profiling being based on the use of statistics, there is a real probability that a given characteristic will be wrongly attributed to an identifiable or identified individual. In extreme cases, individuals may be deprived from accessing vital goods and services, such as credit or insurance, or may have to pay a higher price for them. Behavioural pricing is obviously attractive to business. It allows to maximise profits by adjusting the price that a customer has to pay based on data about that customer. The required pricing technology exists and the amount of data available from loyalty programmes, web histories, and increasingly social media networks

has gained widespread acceptance and usage in online advertising.[3] Targeted advertisements are generally more valuable and efficient, providing important revenues, but also more intrusive of privacy rights.[4] As regards the fight against terrorism, the use of blacklists based on statistical inferences is bound to result in non-terrorists being prevented from boarding planes and offers no absolute guarantee that terrorist passengers will be intercepted.

Secondly, the right to privacy implies the existence of different spheres of private life which must be respected by any data processor. Profiling based on data obtained from an individual's Internet use will almost naturally mix data pertaining to separate spheres of private life. Typically, individuals use the same terminal to communicate with their family, employer, friends, doctor, trade union, bank or lover. This means that, in practice, where a general search engine is used, the service provider hosting the search engine has a 'global' view of an identified individual. All this results in what the German Federal Constitutional Court described in its judgment of 2 March 2010 as a diffusely threatening feeling of being watched which can impair a free exercise of fundamental rights.[5]

The recommendation does not call into question the legitimacy of profiling. It states explicitly that the use of such techniques provides benefits for users, the economy and society at large, such as adapting offers to meet demand, permitting an analysis of risks and fraud and assisting law enforcement. But the risks mentioned require effective safeguards against abuse, which cannot rely only on self-regulation. As the European Court of Human Rights has emphasised in many of its judgments, where fundamental values and essential aspects of private life are at stake, state authorities have a duty to establish an effective regulatory and enforcement framework of protection.

Positive obligations under the ECHR may involve the adoption of measures by state authorities designed to secure respect for private life even in the sphere of relations of individuals between themselves, for example an Internet user and those who provide access to a particular website. In other words, there is a positive obligation on the state to ensure an effective deterrent against grave acts to a person's personal data sometimes by means of efficient criminal-law provisions.[6] In the case of *K.U. v. Finland*, the Court highlighted this positive obligation in the context of an Internet-related complaint.[7]

---

[3] "Behavioral Pricing: A consumer's worst nightmare, a merchant's dream," Allen Gannett, last modified 21 January 2012, http://thenextweb.com/insider/2012/01/21/behavioral-pricing-a-consumers-worst-nightmare-a-merchants-dream/.

[4] See the US White paper "Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy", January 2012: 11–12, http://www.whitehouse.gov/sites/default/files/privacy-final.pdf

[5] Federal Constitutional Court, judgment of 2 March 2010, 1 BvR 256/08, 1 BvR 263/08, 1 BvR 586/08, http://www.bverfg.de/entscheidungen/rs20100302_1bvr025608.html

[6] *X and Y v. the Netherlands*, judgment of 26 March 1985, §§ 23–24 and 27, Series A no. 91; *August v. the United Kingdom*, decision of 21 January 2003, no. 36505/02; and *M.C. v. Bulgaria*, judgment of 4 December 2003, no. 39272/98, § 150.

[7] *K.U. v. Finland*, judgment of 2 December 2008 (no. 2872/02), § 43.

16.3 Definitions and Impact on the Right to Privacy

The recommendation defines "profiling" as an automatic data processing technique that consists of applying a "profile" to an individual, particularly in order to take decisions concerning him or her or for analysing or predicting his or her personal preferences, behaviours and attitudes. A "profile" denotes here a set of automatically generated data characterising a category of individuals that is intended to be applied to an individual.

There are usually three profiling stages. The first stage consists of large-scale collection of usually anonymous data on individual behaviour. This may be a shopping basket, a telecommunications bill or a list of train journeys. During the second stage, data undergo computer analysis to correlate certain behavioural characteristics. Invisible to the naked eye, computing power and the sophistication of algorithms bring to light correlations, without any interference by human logic or common sense. In the third stage, this correlation is applied to an identified or identifiable individual.

The recommendation starts from the premise that individualised profiles thus generated are not so anonymous as sometimes pretended or assumed. It covers, even if only incidentally, the collection and processing of anonymous data in as much as the processing of these data in the first and second stages may be crucial in determining the legitimacy and security of processing of personal data in the third stage. In reality, the three stages constitute a continuous process.

Applying profiling techniques, the web-browser editor, the cyber-marketing company or a website can thus be involved in the processing of personal data. While the information contained in profiles may be considered objective and irrefutable, their processing through automated means allows data controllers to go well beyond neutral identification.

Whenever personal data is being processed, both Convention 108 and the ECHR are fully applicable. In *S. and Marper v United Kingdom*, the European Court of Human Rights held that, "[T]he mere storing of data relating to the private life of an individual amounts to an interference within the meaning of article 8."[8] In the online world, the individual contact point (a PC, cell phone or tablet) no longer necessarily requires the disclosure of a person's identity in the traditional sense. As also recognised by the Court of Justice of the EU, internet protocol addresses constitute "protected personal data".[9]

The recommendation's preamble refers in particular to the linking of a large number of individual, even anonymous, observations, which places people in

[8] *S. Marper v U*K, judgment [GC] of 4 December 2008, § 67. See already *Amann v. Switzerland*, judgment of 16 February 2000.

[9] *Scarlet Extended SA v Societe belge des auteurs, compositeurs et editeurs* ("SABAM"), Case C-70/10, judgment of 24 November 2011, § 51.

predetermined categories, very often without their knowledge. When attributed to a data subject, such profiles make it possible to generate new personal data which are not those which the data subject has communicated to the controller or which he or she can reasonably presume to be known to the controller.

16.4 Drafting of the Recommendation and Its Legal Effects

The committee of experts established under Convention 108 (T-PD) started its work on profiling in 2008. The committee is composed of representatives from all states parties to the Convention (at the time 41, now 43). Observers from the European Commission, the International Chamber of Commerce and the French speaking association of data protection authorities among others, also contributed to the work with their expertise. It should be noted that EU member states coordinated their position throughout the negotiations. It was thus ensured that the resulting text fully conforms with the relevant EU legislation, in particular Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

During the drafting process, public consultations were held on different drafts of the recommendation and comments were sought from various stakeholders such as Internet access providers, associations of online advertisers and representatives of trade and consumers' associations. The text remained, however, controversial among them, with the ICC opposing its adoption because it considered that it did not sufficiently take into account the technological and business reality as well as economic impact on, and application to, various sectors.

On 23 November 2010 the recommendation was eventually adopted by the Committee of Ministers, representing the governments of all 47 Council of Europe member states. Only the United Kingdom reserved the right to comply with it or not.[10] Addressed to the governments of member states, it contains principles and guidelines to be implemented through national legislation and self-regulation. It pursues three main objectives:

- to provide a coherent normative framework to be used by national regulators;
- to ensure effective protection of the rights of data subjects striking a fair balance between the protection of privacy and the legitimate interests of advertisers and consumers or the public at large;
- to avoid that individuals are being subjected to decisions – or even worse, discrimination or stigmatisation – automatically, on the basis of mere profiles.

Though not a treaty itself, the recommendation has legal effects. Firstly, it must be seen as a further development of the general principles of Convention 108,

[10] In accordance with Article 10(2)(c) of the Rules of Procedure of the Ministers' Deputies.

applying them to the use of profiling techniques. Secondly, the European Court of Human Rights regularly refers to Convention 108 and relevant Committee of Ministers' recommendations in its case-law relating to data protection under Article 8 ECHR.[11] The recommendation's standards are thus directly relevant for the interpretation and application of the ECHR. In this way, some of the soft-law standards developed by expert committees are integrated into the respective ECHR provisions, thereby acquiring added legitimacy and above all legally binding force. Integrating these new elements in its case-law helps the Court to keep its case-law in line with developments and commonly accepted standards of European societies. The Court's approach is consistent with the idea of the Convention as a living instrument that must be interpreted in the light of present-day conditions. Finally, the recommendation may also gain legal effects through the case-law of national courts and the decision making of national data protection authorities.

16.5 Conditions for the Use of Profiling Techniques

The recommendation starts by requiring member states:

- to guarantee respect for fundamental rights and freedoms whenever profiling techniques are used, notably the right to privacy and the principle of non-discrimination;
- to encourage the design and implementation of procedures and systems in accordance with privacy and data protection, already at their planning stage, notably through the use of privacy-enhancing technologies ('privacy by design').

The recommendation further requires that collection and processing of personal data in the context of profiling may only be performed if it is provided for or permitted by law. These references to "law" are of course to be understood not as any law, but legislation, including established case-law, in accordance with the principles of this recommendation. Principle 3(4)(b) for example states that profiling requires the consent of the data subject or must be necessary for the performance of a contract or for vital interests of the data subject or legitimate public interests. Any consent shall be free, specific and informed, and in the case of sensitive data it must additionally be explicit.

Today, browser options are configured by default in order to allow third-party cookies. It can be questioned whether this default setting constitutes an expression of free, specific and informed consent.

[11] See for example *S. Marper v UK*, judgment [GC] of 4 December 2008, § 67; *Bouchacourt v. France, Gardel v. France and M.B. v. France*, judgments of 17 December 2009, §§ 26 and 61.

16.6 Rights of Data Subjects

The recommendation foresees the following basic rights of data subjects:

– to receive information including on the purposes and effects of profiling. The explanatory memorandum underlines that "[w]ithout an understanding of these elements there could be no effective exercise of other safeguards – the right to object and the right to complain to a competent authority."[12] For example, persons receiving proposals for insurance against water damage should be informed of the logic followed to calculate the prices quoted. Was their risk profile based on statistics? Which of their personal circumstances were taken into account in calculating the insurance premium?
– to object to the use of their personal data for profiling;
– to object to decisions having legal or other significant effects, including where such decisions are taken in the course of the performance of a contract;[13]
– to obtain from the data controller communication of personal data, the logic underpinning the processing, significance and consequences of the profiles attributed.

16.7 Exceptions

The recommendation allows for exceptions to some of its principles, thus taking a balanced approach, which leaves states a certain margin of appreciation. Since such exceptions will constitute restrictions to the right to private life or other rights under the ECHR, the conditions and safeguards under the ECHR apply, notably the requirement that such measures must be necessary in a democratic society and satisfy the proportionality test applied by the Strasbourg Court.

Under the ECHR, the compilation, storage, use and disclosure of personal information amounts to an interference with one's right to respect for private life as guaranteed by Article 8 ECHR.[14] Such interference breaches Article 8 ECHR unless it is "in accordance with the law", pursues one or more of the legitimate aims referred to in paragraph 2 and, in addition, is "necessary in a democratic society" to achieve those aims. In the case of *Uzun v. Germany*,[15] the Court came to the conclusion that the applicant's surveillance via GPS, ordered by the Federal Public Prosecutor General in order to investigate several counts of attempted murder for which a terrorist movement had claimed responsibility and to prevent further bomb

[12] Paragraph 140 of the explanatory memorandum.

[13] Compare Article 15 (1) of Directive 95/46/EC.

[14] *Leander v. Sweden*, judgment of 26 March 1987, § 48, Series A no. 116.

[15] *Uzun v. Germany*, judgment of 2 September 2010, no. 35623/05.

attacks, served the interests of national security and public safety, the prevention of crime and the protection of the rights of the victims. In the end, the interference was proportionate to the legitimate aims pursued and thus "necessary in a democratic society" within the meaning of Article 8 (2) ECHR.

16.8 Remedies

The recommendation abstains from prescribing binding standards for sanctions and remedies. It merely sets out the principle that domestic law should provide for appropriate sanctions and remedies, leaving it to national legislation to fix precise amounts. In this context, it is worth mentioning that, for example, German legislation on scoring enacted in 2009[16] provides for penalties of up to €300,000 if the interests of data subjects are harmed through wrongful use of data (processing, profiling) or denial of information.

16.9 Data Security

Appropriate technical and organisational measures will be required to guard against accidental and unlawful destruction and loss of data as well as unauthorised access, alteration, communication or any other form of unlawful processing. The appointment of an independent person responsible for the security of information systems is required as well as specific measures to prevent re-identification of data subjects through the use of aggregated statistical results.

16.10 Conclusion

The drafters of the recommendation are not privacy zealots. They recognise that profiling pursues legitimate interests. But the example of online advertising clearly shows that there are so many grey areas that if the end-users were aware, it would turn their hair grey.

We are convinced that more transparency is in the interest of all. If Internet service providers, research and online advertisement companies care about the long-term success of their business, they should take an active role in informing their customers about the purposes and effects of profiling. This is why the recommendation also promotes self-regulation, not as a substitute for, but in addition to, domestic legislation.

[16] See Section 43 of the Federal Data Protection Act (Bundesdatenschutzgesetz; BDSG).

References

Council of Europe. 2012a. Council of Europe convention 108. http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=108&CM=8&DF=19/01/2012&CL=ENG. Accessed 27 Feb 2012.

Council of Europe. 2012b. Council of Europe recommendation CM/Rec(2010)13. https://wcd.coe.int/ViewDoc.jsp?id=1710949&Site=CM. Accessed 27 Feb 2012.

Council of Europe. 2012c. Rules of procedure of the Ministers' Deputies. https://wcd.coe.int/ViewDoc.jsp?id=814763&Site=COE. Accessed 27 Feb 2012.

European Court of Human Rights. 2012. HUDOC database. http://www.echr.coe.int/ECHR/EN/Header/Case-Law/Decisions+and+judgments/HUDOC+database/. Accessed 27 Feb 2012.

Federal Commissioner for Data Protection and Freedom of Information. 2012. The "Federal Data Protection Act" "Bundesdatenschutzgesetz" (BDSG). http://www.bfdi.bund.de/EN/DataProtectionActs/Artikel/BDSG_27idFv01092009.pdf?__blob=publicationFile. Accessed Feb 2012.

Federal Constitutional Court. Judgment of March 2, 2010, 1 BvR 256/08, 1 BvR 263/08, 1 BvR 586/08. http://www.bverfg.de/entscheidungen/rs20100302_1bvr025608.html

Next Web. 2012. The behavioral pricing: A consumer's worst nightmare, a merchant's dream. Last modified 21 Jan 2012. http://thenextweb.com/insider/2012/01/21/behavioral-pricing-a-consumers-worst-nightmare-a-merchants-dream/

Walter, Jean-Philippe. 2011. *Le profilage des individus à l'heure du cyberespace: un défi pour le respect du droit à la protection des données.* Datenverknüpfung: Problematik und rechtlicher Rahmen, Zürich: Schulthess. 87–114.

White House, The United States' White paper. 2012. *Consumer data privacy in a networked world: A framework for protecting privacy and promoting innovation in the global digital economy*. January, 11–12.

http://www.whitehouse.gov/sites/default/files/privacy-final.pdf

Part V
Case Studies

Chapter 17
Communicating Privacy in Organisations. Catharsis and Change in the Case of the Deutsche Bahn

Daniel Guagnin, Carla Ilten, and Leon Hempel

17.1 Introduction

This contribution presents an analysis of the fundamental transformation of the Deutsche Bahn corporation (DB) with regard to privacy and data protection policy and implementation. We will argue that the scandal-afflicted organisation has started approaching data protection implementation as a problem of *communication* and *negotiation*. Its development shows first successes in regaining trust and improving protection through massive efforts to translate data protection law into day-to-day privacy aware practices.

The case study[1] has been conducted in the framework of the EU-project "Privacy Awareness through Security Organisation Branding". The project performed an

[1] The present case study is a composite analysis from a number of activities – both structured and informal – over the course of the PATS project (2009–2012). In detail, it is based on conversations between the authors and Data Protection Authorities as well as privacy activists who were involved in the present case as well as conversations conducted with DB staff in different contexts; more supporting material was acquired through own online research and media analysis. The analysis must not be read as a definitive representation of the current situation at the Deutsche Bahn, but should be understood as a case-inspired conceptual contribution.

D. Guagnin (✉)
Centre for Technology ans Society (CTS), Technical University of Berlin,
Seelower Str. 1, 10439 Berlin, Germany
e-mail: guagnin@ztg.tu-berlin.de

C. Ilten
Department of Sociology, University of Illinois at Chicago,
1007 West Harrison Street (MC 312), Chicago, IL 60607-7140
e-mail: cilten2@uic.edu

L. Hempel
Centre for Technology ans Society (CTS), Technical University of Berlin,
Alt-Moabit 82, 10555 Berlin, Germany
e-mail: hempel@ztg.tu-berlin.de

S. Gutwirth et al. (eds.), *European Data Protection: Coming of Age*,
DOI 10.1007/978-94-007-5170-5_17, © Springer Science+Business Media Dordrecht 2013

analysis of privacy awareness in security-related organisations and of their security and privacy communication in six countries.[2] One important insight from the interview processes is that a paralysing silence governs security markets when it comes to privacy protection. While actors acknowledge that it is a challenge to translate data protection law into practice, they have no incentives to become more active about these problems.[3]

Building on PATS initial assumption that self-regulation in this field could be fuelled by communication – more specifically, "branding" as an act of self-presentation and improvement – we inquired about the possibility of more public communication by these companies. This concept of a proactive, ongoing effort by data controllers to manifest their compliance is akin to the rekindled discourse around accountability.[4]

In line with the accountability idea and linked discussions, we have argued that privacy protection needs to become a reflexive ongoing process within the data controlling organisation. This self-critical process is the basis for an increasing awareness about privacy issues and the starting point for implementing effective structures of accountability to ensure good privacy practices. What the project initially targeted with the use of the term "branding" can be understood as a complex of communication, both within organisations and into society.[5]

The case of the Deutsche Bahn exemplifies the role of communication in bridging the gap between law and practice. The corporation underwent massive scandal due to the surveillance of employees well into their private lives on a systematic basis. After experiencing complete image calamity, the organisation implemented a potent

[2] PATS partners include the UK, Israel, US, Poland, Finland, and Germany. The project is funded under the EU FP7. Further information and related reports and publications can be found on www.pats-project.eu

[3] Cf. Carla Ilten et al., "How Can Privacy Accountability Become Part of Business Process?" *Privacy Laws and Business International*, no. 112 (September 2011): 28–30.

[4] Recent contributions to the accountability discourse can be found in the book "Managing Privacy through Accountability", ed. Daniel Guagnin et al. (Palgrave Macmillan, 2012 forthcoming): Joseph Alhadeff et al., "The Accountability Principle in Data Protection Regulation: Origin, Development and Future Directions."; Colin Bennett, "The Accountability Approach to Privacy and Data Protection: Assumptions and Caveats.". From the European Commission see "Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions – A Comprehensive Approach on Personal Data Protection in the European Union." (2010) and Article 29 Working Party. "Opinion 3/2010 on the Principle of Accountability", (2010). The debate is also outlined in Daniel Guagnin et al., "Privacy Practices and the Claim for Accountability." In *Towards Responsible Research and Innovation in the Information and Communication Technologies and Security Technologies Fields*, ed. René Von Schomberg. (Luxembourg: Publication Office of the European Union, 2011).

[5] On the basis of our results, we have developed a privacy branding model which you can find in detail at the project website pats-project.eu, see also Daniel Guagnin et al.. "Bridging the Gap: We Need to Get Together." In *Managing Privacy Through Accountability*, ed. Daniel Guagnin et al. (Palgrave Macmillan, 2012).

data protection infrastructure whose primary asset is (wo)manpower: over the course of an entire year, employee and employer representatives, board members and personnel managers were involved in negotiating the new DB privacy and data protection policies. In this process, a new organisational data protection infrastructure has been created. Another year saw an extensive process employee training and communicating the achievements to the workforce. What is more, new approaches to dealing with the translation of policies into practice are experimented with. Again, these consist mainly of communication on an ongoing basis in a trusting atmosphere between workforce and data protection officers, as we will show.

17.2 Scandal

Even though it is likely known to the reader what happened at the Deutsche Bahn, we will briefly sketch the story of one of the biggest scandals revolving around privacy infringement and data protection failure.

In 2009, it became public that employees – hundreds and thousands of them – had been surveilled and researched by external agencies, Network Deutschland GmbH in particular, by order of DB staff. Over the course of months, more and more details about the extent of the spying and data exchange came to light: not only employees, but their spouses as well had been investigated with regard to their private finances including money transfers, travels, online behaviour, and biographical data, among others. The orders to establish these data have been given orally by DB members in charge of "fighting corruption", and sums as large as € 800.000 were agreed on without formal documentation.

The surveillance affected all levels of employees – works council members as well as managers. The substance of the infringing activities makes this a real privacy issue – not just one of careless data loss. While data protection is often equated with data security, this case reminds us that privacy starts with the non-existence of data rather than their protection. The private lives of employees have been illegally intruded for purposes of control and internal policing, over the course of years.[6]

Such systematic surveillance is not the failure of an individual. Rather, an entire network within the corporation was involved in this attempt at managing the DB through finding its "black sheep" – critics of the stock launch so fervently put forward by CEO Hartmut Mehdorn, for example, who were suspected of handing information to the media. In a sense, Mehdorn and those engaging in the surveillance activities were trying to control the information flow about the corporation by controlling employees.

[6] For a discussion of how privacy and data protection are differently legally defined see Raphaël Gellert and Serge Gutwirth, "Beyond Accountability, the Return to Privacy?" In *Managing Privacy through Accountability*, ed. by Daniel Guagnin et al. (Palgrave Macmillan, 2012).

Needless to say, the DB data protection scandal caused a complete loss of trust among the majority of the workforce as well as a good measure of anger. The atmosphere was more than stormy – something drastic needed to happen in order to create clean air.

17.3 Catharsis

As we have observed in the PATS interviews on privacy awareness in the security field, companies find different answers to dealing with scandal. Companies can react with retreat, or they can emerge and attempt to re-cast their image. With regard to the public, this seems to be a fight-or-flight decision for organisations – depending on what is at risk or can be gained in the situation.

Obviously, a scandal of the scope as described for the DB is nothing that can be pushed aside easily. The scandal and CEO Mehdorn's personal involvement kept the media busy for months. The criminal espionage activities concerned the workforce, which means that next to the public and stakeholders, the very base of a fairly traditional organisation had lost their trust in the company and demanded consequences.

Secondly, the activities were closely tied to the politics of the DB future development and Mehdorn's iron vision of a stock-noted corporation. The scandal seemed to be born out of an authoritative style of management, and nothing about it was negligible or laissez-faire. In addition to the surveillance of workforce, a related affair of media manipulation with regard to the issue of a possible stock market launch and to union strikes became public.

Real personnel consequences were imperative. CEO Mehdorn, a powerful and adamant leader, had to offer his resignation in March 2009. The new CEO Rüdiger Grube consequently exchanged most of the top management, who proved to be intensely involved in the affair. The representatives of corporate security, auditing, and anti-corruption had to leave. Massive organisational restructuring followed, including the creation of a Board-level Department for Compliance, Legal, Data Privacy and Security which also hosts the new data protection officer, as we will lay out in detail below.

Lastly, a monetary penalty was imposed on the DB through the Berlin state data protection officer, Alexander Dix. It was the largest sum ever inflicted in the legal area of data protection in Germany – over €1.1 million, which were paid by the DB without objection.

As a corporation of public interest – being the railway provider and completely state owned - catharsis needed to happen for the DB in order to become worthy of the trust of both the public, policy makers, clients, and most of all, its employees. The act of renewal of the top management was an important instance of "purging" the responsible actors, preparing the ground for change. As in Greek drama, the public took part in this catharsis as an audience which was delivered shameful news on a daily basis – the loss of privacy became public, palpable for everyone. Outrage and punishment made for relatively clean air after the foul weather.

17.4 Change: "A new era"

While catharsis is strongly connected to symbolic events and public communication, real organisational change takes place not only in structures, but in the knowledge, attitudes and everyday activities of employees. In conversations about the DB case, there is a clear before-and-after rhetoric with regard to catharsis: a new era has begun.

In the case of the DB, scandal affected employees' trust in the corporation in particular since the spying was directed at workforce, who demanded change vocally – an internal problem. Accordingly, catharsis needed to be communicated both outwards and inwards by the organisation.

The following process of change that will be described now is a slow and profound one; it is about regaining trust and including as many actors as possible. It is about communicating privacy. We will first describe the formation of the corporate works agreement, which itself is the outcome of a yearlong process of communication within the DB. Next, we will reproduce how this agreement was communicated to all members of the DB.

17.4.1 The Corporate Works Agreement

17.4.1.1 Negotiating the Agreement – An Act of Communication

The Corporate Works Agreement ("Konzernbetriebsvereinbarung", KBV) is the outcome of one year of negotiation between representatives of different levels of the DB and has been adopted in November 2010. After the 2009 data protection affair had revealed all the details of employee surveillance and spying practices, a "poisoned atmosphere" impregnated the whole corporation. Initially, a lot of tension was felt in the discussions and negotiations about how to put new data protection mechanisms in place. It was even a challenge to find common language for a mutual understanding. The KBV was mainly negotiated by a working committee called "Employee Data Protection" which incorporated representatives of employers and employees, the central works council, the human resources department, subsidiaries and the data protection office.

The whole process of negotiation was essential for regaining the trust of the employees. Thus the negotiations themselves were a process of building mutual understanding and communication. The fact that the KBV was completed in this way led to appreciation on the part of employees – after all the unpleasantness, something was happening. The data protection office made a point of actively communicating that data protection is not only about protecting bits and bytes but about human beings. In other words, privacy is not only about secure data storage and transfer but first of all restricting the data sets about human beings (principle of data economy). This message was addressed to employer stakeholders especially. The active communication of these concepts can be understood as a measure of awareness building.

17.4.1.2 Beyond Law, Towards Accountability

Since the KBV was developed in the dire need of regaining trust and was negotiated by different stakeholders, the outcome is far beyond simple compliance with data protection law. While the agreement is naturally based on legal frameworks, it has in fact a progressive character and anticipates potential changes imminent with the amendment of German data protection law which is ongoing. Moreover, the agreement may even provide an example for solutions with regard to the claim for accountability which has regained importance over the past years.

The agreement can be understood as a reflexive definition of the future data protection practice of the Deutsche Bahn. It is a prospective declaration; a manifest of how privacy practices shall be organised and implemented.[7] The next section will shortly outline the structural changes in the organisation of data protection which are initiated by this agreement.

17.4.2 New Actors and Structures – Implementing Accountability

In this part, we will outline the structural changes that have been made with regard to data protection at the DB. To contrast the restructuring with the earlier set-up, we will firstly sketch the structure before the éclat in 2009.

A central data protection office was in place for the whole group with one Group Data Protection Officer (GDPO) and five assistants. Besides, there were about seventy "contact persons" in the different business areas, especially in business areas where data protection was of high relevance. For these contact persons, data protection activities were an addition to their normal tasks. They were trained internally and their main function with regard to data protection was to be a contact person for the GDPO – not the data processing employees. In practice, they had relatively little data protection expertise and were hardly involved in discussions about changing processes and procedures in the different business areas. Instead, the GDPO negotiated issues with the management of the respective business areas, and the "contact persons" were informed after the fact.

A few more random DPOs existed at some of the DB group companies. However there was no real framework for interaction between these different data protection instances. In this set-up, the officers were not entirely independent. Tellingly, a substantial overview of the DPOs in place was only gained in the process of restructuring. Seen that this represents the entire organisational structure of privacy and data protection for a corporation with a +200.000 workforce, the status of data protection

[7] The Corporate Works Agreement "Employee Data Protection" can be downloaded at http://recht.verdi.de/beschaeftigtendatenschutz/data/Konzernbetriebsvereinbarung.pdf (German) [last accessed 1.3.2012].

before 2009 is clear. The lack of elaboration, independence, and interaction between data protection bodies shows that it was not considered a significant issue by the management.

When the working committee "employee data protection" was installed, they realized that they would have to define new and more effective organisational structures. A first challenge was finding the adequate number of people in charge of data protection. On the one hand, the first goal was to provide the employees the best support possible, on the other hand the corporate structure of the DB needed to be integrated in order to keep the office visible and manageable. While a great number of new data protection experts were installed, their distribution and number needed to be balanced carefully – especially with respect to an easy mutual communication between the representatives and a common understanding.

The first action to strengthen the organisational data protection structure at the DB was to enhance the top level group data protection office. The office, headed by the GDPO Ms Newiger, got five departements with dedicated functions: Client and employee data protection got one department each, additionally one department for audits have been set up and two departments for the management of the decentralized data protection structure of the whole group, split into business areas. The GDPO is responsible for the group and subsidiaries except for five more DPOs which are assigned to subsidiaries.[8] All the DPOs are independent and instruction-free from the management or other levels of organisation. This line of six DPOs is the top level of full-time independent DPOs.

The DPOs' competences include controlling the correct processing and application of personal data software, ensuring that employees processing personal data are adequately trained for compliance with the legal provisions; and evaluating automatic data processing systems with regard to whether they constitute a risk to the rights of the concerned data subjects.

Next to the top level, it was deemed important to install a secondary structure of trained assistants which operate in the several business areas of the corporation. At this next level, ten highly skilled "Trained Assistants for DP" have been introduced whose competences are comparable to the DPOs. They receive the same training and are dedicated to DP tasks full-time. Their assignment relates to the specific DP issues of their business area. In their function of DP Assistant, they are granted a special employment protection which exceeds the end of their activities as DP Assistant by a year. The assistants are instructed by and regularly meet up with the central data protection office, and are legally part of the subsidiary they are employed in.

In addition to the levels Group DPO, DPOs and Assistants, another category of "Data Protection Confidants" has been created. Data Protection Confidants are instructed by the Trained Assistants for DP. They may be assigned other duties besides their Data Protection tasks, but it is defined that their tasks related to Data Protection issues are first priority. The Data Protection Confidants report to the

[8] See http://recht.verdi.de/beschaeftigtendatenschutz/data/Konzernbetriebsvereinbarung.pdf

Trained Assistants and are charged with conducting monitoring in their Business Areas, as well as with giving feedback to the Group DPO and the corporate management and to report Data Protection violations.

In all, there are currently more than a hundred Data Protection Confidants assigned to represent the Data Protection Office broadly in the whole national DB group corporation. The time split between Data Protection and other tasks is a challenging question and the Corporate Works Agreement offers definitions that help employees dedicating enough time to these purposes. Models for calculating the exact amount have been discussed. It is generally agreed that work in committees, trainings, travels and similar educational time uses are a necessary part of this assignment.

All employees charged with Data Protection tasks on all levels enjoy the training by the German Association for Data Protection and Data Security (GDD) who provides official certification. The GDD is an independent association which builds expertise and provides training and other services with regard to data protection. It is highly recognized by the authorities and proved to be the only organisation capable of handling the mass demand for trainings in such a short time frame for the DB. A total of about 150 employees has been trained until now.

The dimensioning of the data protection infrastructure will be tested over the next years and revised if needed. The current situation thus represents the first approach by the Data Protection Working Group. While there are calls for a "return on investment" by some management actors, it is generally expected that the basic new structure of DPOs and Trained Assistants will be preserved in any case.

To sum up, the restructuring of the organisational structure and competences must be evaluated as a giant leap in terms of both numbers and quality. The new infrastructure comes as a huge investment and is extremely visible both within the company and to the public.

Next to building these structures in working groups and through the collective process of creating the KBV, the most important step in regaining trust within the company was to communicate these changes to the workforce at large. In the case of the DB, creating and communicating the changes went hand in hand. Translating the formal rules into practice has become pretty much a public affair within the DB, as the following section will outline.

17.4.3 Spreading the News: Communication

The training of the data protection officers, trained assistants and confidants was a considerable instance of communication, a process which started in March 2011 and is nearly finished. In the direction of the workforce, a communication concept which aims at spreading the message about the new era of data protection in detail has been devised. It was understood that the new KBV would unfold the greatest impact if the changes and the progress made were understood by all employees.

The first step in this process of communication was to conduct six regional conferences with about 3,000 attendees. Executives, stakeholders, personnel managers and data protection representatives were invited. The management board was present with one or two representatives, and chairpersons of the trade unions and working council attended. Due to the kick-off meeting character of the conferences, it was not possible to address all questions, rather the event conveyed the general turn of the DB data protection policy. Among the employees, a high demand for participation was reported.

Consequently, smaller regional workshops with about 30 attendees were conducted by the human resources department, the trade union and the central data protection office. There, after a short presentation of the data protection policies and the Corporate Works Agreement, the attendees were split into groups to collect questions and concerns which were then discussed in 1 day workshops. In this context employees had the opportunity to find out what the KBV means in the very practice of everyday activities.

The DB has an infrastructure of regional networks in place where personnel managers of the different business areas in each region meet to balance their interests for a joint go ahead. These networks have been used by the central data protection office to spread the changes to the business areas. This way, the personnel staff could discuss their questions and concerns in a confidential sphere, and dialogue between different stakeholders (working council, unions, and management personnel) was opened up.

The regional workshops were met with large demand as well. In 2011 all workshops were booked out and follow-up workshops are planned for 2012. The feedback from the workshops was quite positive, criticism is mostly voiced about the practice relevance of the instruction material. The translation between theory and practice is still difficult and leaves attendees stating that a follow-up seminar with more example cases would be welcomed. This shows the importance of Data Protection staff – rather than policy texts – within the organisation. People need contact persons to discuss their practice cases. A single document such as the KBV is an important milestone, but does not accomplish the translation into practice by itself. Structures of accountability need to be defined, but these structures need to enable continuous communication to take effect in organisational practice.

For the DB change process, this means that after the phase of creating the new data protection infrastructures, the continuation of communicating privacy needs to be organised. To this end, data protection jour fixes are installed where every 2 months data protection representatives of all levels come together to discuss standards and upcoming issues. These meetings are intended to stimulate communication between the data protection representatives and at the same time support the diffusion of data protection related issues to the work force. This process of dissemination is still unfolding.

Beyond these events of personal communication, broadcast communication has been set up through an online information platform on the DB Intranet. Supporting guidelines have been published in print. The internal print media are also used to communicate the changes achieved through the KBV. Step by step, the new data protection policy is presented and translated for the workforce.

On a more general level, the DB has set up an accessible procedure for whistle-blowing in all compliance matters. This includes privacy and data protection issues and is a measure of empowerment for the workforce.

While there are no official or formal tools that are used for measuring the effect of communication on trust or the general atmosphere among the employees, the many communication events lead to a fairly good sense of "atmosphere" for the data protection representatives involved.

17.5 New Experiences: Bridging the Gap

The above-described intense measures of communication and the related employees' reactions provide us with valuable insights into the difficulties of bridging the gap between law and practice. Data protection regulation is a legal area that comes with some latitude. There is black and white, but only rarely – between them lies the margin of discretion – which has been narrowed the KBV, but still it takes an individual case assessment most of the time.

It is this process of *translation* from rule to action, as we have called it elsewhere,[9] that makes privacy and data protection so complex. There is no denying that in order to implement data protection effectively, resources need to be dedicated. What these resources consist of, though, is a concept that is changing: the translation of law into practice calls for human translators who provide support on an ongoing basis. The problematique of data processing inside and outside of standard systems in a large organisation exemplifies this line of thought.

17.5.1 Data Within and Outside of "IT standard systems"[10]

In a large corporation like DB, IT systems are fairly standardised and well-defined, but with the same token also limited. In general, these kinds of configuration lead people to start operating outside the standard system for simple purposes. Operating outside standard IT systems, though, means that all security and data protection standards devised for the standard systems will also be circumvented. The mere set up of a simple Excel table for the purposes of making a list of participants for an event could legally become a matter of consent through the works council when it is done outside of standard systems of data processing[11] – a rule that can become highly hindering in many everyday situations that seem innocuous.

Simply circumventing rules, however, re-creates the well-known gap between law and practice. If rules were to be implemented perfectly, all processes would be

[9] Guagnin et al., "Bridging the gap"op. cit.

[10] This section reflects on §9 of the Corporate Works Agreement, "Nebendatenverarbeitung".

[11] cf. §9 of the Corporate Works Agreement, op. cit.

defined. In the described situations of conflict, it means that processes that move at the margins of these rules and are not yet defined *within* them either need to be carried out in secret – or become (re-)defined.

In conversations we had about this topic, the complexities and difficulties of putting data protection law into practice in everyday business going on were acknowledged within the DB. Compared to our earlier research on privacy awareness in security-related companies, this is a massive step forward from a dead quiet to an acknowledgement.

If a procedure is sufficiently desirable to be included in the standard system, a lengthy path of legalisation needs to be embarked on: the procedure must be specified, DPOs, councils of different units and the works council have to be consulted before the new procedure can be adopted. It has been recognized, though, that this path of legalisation is an intensive one: it can take up to two years until a procedure is finally defined. In practice, it follows that operations outside the standard systems do and will happen – but this reality can be handled either blindly, or in a reflected fashion. "At least ask your works council", is the simple, but effective attitude voiced about this: do not operate in silence. Communicate your needs and problems.

17.5.2 Solutions in Practice Require Communication

This need for *un-silence* is particularly strong still in the aftermath of scandal. There seems to be a very high demand for information and a "not yet quite relaxed" atmosphere, especially on the part of the management, which has seen colleagues fired.[12]

These challenges are at the heart of conversations about data protection developments: changing the procedure of *deciding about procedures*. Put differently, the hope voiced is to be able to converge rules and practice on an ongoing basis – whenever insecurities arise. This means, of course, that considerable time will be invested in these decision-making processes and that sometimes business processes will be slowed down. The first step is already a big task: the directory of procedures needs to be compared to real practice and adapted so that all activities are well documented.

On the upside from the point of view of the corporation, assuming that rules can be adapted to better grasp the content of actual business activities, a gain in efficiency can be expected over the course of a few years. Most importantly, rules will then be known to all the actors involved; practices will be open instead of covert, and actors will likely be more satisfied with the results of negotiated decision making. Lastly, such documented processes of adaptation provide infrastructures of accountability for everyone to revisit.

[12] In an earlier interview with a security association representative, we have heard a similar judgement: "The day that Mehdorn had to leave – that's when the managers knew that this topic can turn into their problem."

Of course, with such vast changes, there is criticism as well: while the new structures in place are considered adequate by most, the cost question has come up, as well. Clearly, the risks associated with data protection failure are not easy to assess (even though the penalty inflicted on the DB was very concrete), and benefits in trust and atmosphere are even more intangible. Taking into account the conclusions about *measuring the atmosphere*, however, it seems beyond question that the effects of the new data protection structures and communication are tangible, indeed, even if not in quantitative figures.

17.6 Conclusion: Putting Data Protection to Practice Is a Process of Communication

In this chapter, we have argued that the translation of privacy and data protection law into organisational practice must be understood as a process of communication. Building on our earlier findings about massive gaps between data protection law and practice in the security sector, we have analysed the case of the Deutsche Bahn, which underwent scandal and subsequently reorganised its privacy and data protection infrastructure fundamentally.

The case exemplifies the role of communication as an ongoing process of rule negotiation, implementation of structures, and knowledge transfer in organisations. Data protection law as it is codified is not a plug-and-play device – the legal text needs to be translated with respect to every activity carried out in a company. The DB has recognized this challenge and – in the aftermath of major failure – has moved through an extensive process of negotiating the new formal rules for privacy protection in the company, as well as communicating them to as many employees and managers as possible.

The goal of this process is not to end up with a static set of rules and responsibilities that take care of data protection once and for all, but to rebuild trust within the organisation and find ways to deal with insecurities in the future – openly. The fact that insecurities exist and will always emerge as a function of business activities and technological changes is entirely acknowledged and reflected in new approaches, as the discussion of data processing inside and outside of standard systems has shown. Translation is becoming a regular task, and communication is its method.

References

Alhadeff, Joseph, Brendan Van Alsenoy, and Jos Dumortier. 2012. The accountability principle in data protection regulation: Origin, development and future directions. In *Managing privacy through accountability*, ed. Daniel Guagnin, Carla Ilten, Leon Hempel, Inga Kroener, Daniel Neyland, and Hector Postigo. New York: Palgrave Macmillan.

Article 29 working Party. 2010. Opinion 3/2010 on the principle of accountability. URL: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp173_en.pdf. Last accessed 1 Mar 2012.

Bennett, Colin J. 2010. International privacy standards: Can accountability be adequate? *Privacy Laws and Business International* 106: 21–23.

Bennett, Colin J. 2012. The accountability approach to privacy and data protection: Assumptions and caveats. In *Managing privacy through accountability*, ed. Daniel Guagnin, Carla Ilten, Leon Hempel, Inga Kroener, Daniel Neyland, and Hector Postigo. New York: Palgrave Macmillan.

European Commission. 2010. Communication from the commission to the European parliament, the council, the economic and social committee and the committee of the regions – A comprehensive approach on personal data protection in the European union. URL: http://ec.europa.eu/health/data_collection/docs/com_2010_0609_en.pdf. Last accessed 1 Mar 2012.

Gellert, Raphaël, and Serge Gutwirth. 2012. Beyond accountability, the return to privacy? In *Managing privacy through accountability*, ed. Daniel Guagnin, Carla Ilten, Leon Hempel, Inga Kroener, Daniel Neyland, and Hector Postigo. New York: Palgrave Macmillan.

Guagnin, Daniel, Leon Hempel, and Carla Ilten. 2011. Privacy practices and the claim for accountability. In *Towards responsible research and innovation in the information and communication technologies and security technologies fields*, ed. René Von Schomberg. Luxembourg: Publication Office of the European Union.

Guagnin, Daniel, Leon Hempel, and Carla Ilten. 2012a. Bridging the gap: We need to get together. In *Managing privacy through accountability*, ed. Daniel Guagnin, Leon Hempel, Carla Ilten, Inga Kroener, Daniel Neyland, and Hector Postigo. New York: Palgrave Macmillan.

Guagnin, Daniel, Leon Hempel, Carla Ilten, Inga Kroener, Daniel Neyland, and Hector Postigo (eds.). 2012b. *Managing privacy through accountability*. New York: Palgrave Macmillan.

Ilten, Carla, Daniel Guagnin, and Leon Hempel. 2011. How can privacy accountability become part of business process? *Privacy Laws and Business International* 112: 28–30.

Chapter 18
The End of Independent Data Protection Supervision in Hungary – A Case Study

András Jóri

The Hungarian data protection authority (the Parliamentary Commissioner for Data Protection and Freedom of Information) was founded in 1995, shortly after the fall of communism. After 16 years of mostly successful activity in the field of promoting and enforcing information rights, the lawmaker abolished the office, and terminated my mandate as commissioner as of 1st January 2012. In this article I, as the last Commissioner (elected in September 2008), give a short description of the case and argue that this measure was in breach of Directive 95/46/EC, as well as the Hungarian constitution.

18.1 Status quo ante: Parliamentary Commissioner for Data Protection and Freedom of Information

The first data protection act in Hungary was passed in 1992,[1] the Data Protection Authority (DPA) in Hungary was also founded in 1992. The first Commissioner for Data Protection and Freedom of Information was elected in 1995. It was the first body in Europe having competences in both the areas of data protection and freedom of information supervision; the Hungarian lawmaker followed the institutional model of the institutional model introduced in provinces and territories of Canada. Since then, many European countries (Germany (federal level and several *länder*), the United Kingdom, Slovenia, Serbia, Estonia) have combined responsibilities for both areas in one central regulatory authority.

[1] Act No. LXIII of 1992 on the protection of personal data and the publicity of data of public interest.

A. Jóri (✉)
Dataprotection.eu Kft, Gyöngyvér u. 37, 1029 Budapest, Hungary
e-mail: andras.jori@dataprotection.eu

S. Gutwirth et al. (eds.), *European Data Protection: Coming of Age*,
DOI 10.1007/978-94-007-5170-5_18, © Springer Science+Business Media Dordrecht 2013

The Commissioner was elected for 6 years by a two-thirds majority of the Parliament. In effect, that meant that all three commissioners were elected (in 1995, in 2001 and myself in 2008) with the support of all political parties represented in Parliament. While the Commissioner was known in public as the "Data Protection Ombudsman", a closer look at the functions of the this DPA reveals that it was not purely an ombudsman institution; the Commissioner had various tasks and competences, among them educational, consultative and enforcement powers as well.

18.1.1 Functions

Many authors address the question of functions carried out by data protection authorities.[2] In order to be able to better illustrate the changes (or the lack of changes) of the system of Hungarian data protection supervision, three groups of functions can be differentiated.

18.1.1.1 The Commissioner as a Privacy (and Freedom of Information) Advocate

The first function, or rather, group of functions, relate to the role of the DPA as a civil rights advocate; a fierce proponent of information rights aiming to change the legal environment in a way that it gives more room for privacy and transparency. The Hungarian Commissioner was in charge of monitoring the developments in the field of data protection and freedom of information. It had the general obligation to shape the legal environment both at the national and European Union level. For example, each draft act or decree touching upon the protection of personal data or freedom of information had to be sent to the Commissioner for an assessment. At the EU level, the Commissioner, as a member of Article 29 Working Party, was given the opportunity to influence the development of EU data protection law. The Commissioner could also publish general recommendations, setting out interpretations of different acts (based on, primarily, the practice of the Constitutional Court). While these interpretations were not binding but only of a persuasive nature, data controllers, and what is more important, courts, too, usually accepted these opinions. And finally, other activities aiming at changing the landscape (awareness raising projects, organizing conferences, etc) should be considered as part of this function as well.

[2] See Colin J. Bennett 2002.

18.1.1.2 The Commissioner as an Ombudsperson

The second function of the Commissioner was the resolution of conflicts between data controllers and data subjects (in the field of data protection) or between data controllers and citizens submitting FOI requests (in the field of freedom of information) using ombudsman-like powers. The Data Protection Act set out a swift, informal procedure, in which the Commissioner could investigate a case, mediate between the parties, and reach results without the need of complying with all requirements of an administrative course of action. These cases were closed by issuing recommendations (setting out a legal opinion tailored to a given particular case), and made it possible for the Commissioner to deal with conventional conflicts in an effective manner.

In some cases, however, the arising conflicts revealed a drawback of the quasi-ombudsman procedure still in the early years of the institution. Recommendations only worked when the controller was willing to comply with them; and, since they were not binding, the only sanction in cases of noncompliance was "shaming by naming". When good PR was important for a controller, he respected the recommendations of the Commissioner. But, in some instances, these non-binding instruments did not work. For example, those cases involving data controllers that were not well known to the public (thus, bad publicity did not harm their non-existent public image) were particularly problematic. In other cases, controllers were expressly seeking the publicity gained by noncompliance with recommendations of the data protection commissioner. For instance, by publishing shame-lists against the law in the name of "justice", politicians were trying to profit from establishing a "law and order" and "zero tolerance" image of themselves (see more about this case below).

18.1.1.3 The Commissioner as an Administrative Authority (Enforcer)

The third function of the Commissioner was that of an enforcer of data protection law. Some competences relating to this function had been present from the early days, such as the maintenance of the data protection registry. In the field of freedom of information, the Commissioner had the right to issue binding decisions on whether classification of a given piece of information was justified or not; the controller then could challenge the decision of the Commissioner in court. Because of the deficiencies of the pure ombudsman-like procedure shown above, and seeking compliance with the EU Data Protection Directive, the lawmaker further strengthened the order-making powers of the Commissioner in 2003 by giving the DPA powers to order the destruction or blocking of unlawfully processed data.

18.1.2 Independence

The institutional model ensured that only persons enjoying support by a political consensus could be elected for parliamentary commissioner (two-thirds majority

generally could not be reached without a consensus of government and opposition parties). The Commissioner reported to the parliament only and enjoyed immunity similar to that of MPs. These factors resulted in an unprecedented independence in the scene of Hungarian public law and politics, where heads of formally "autonomous" state bodies, e.g. the Financial Supervisory Authority, were regularly replaced after parliamentary elections despite their longer mandates. This independence, and the legitimacy stemming from the election by a qualified majority of MPs, resulted in effective supervision of state data processing activities of state bodies as well as an active role in the field of freedom of information. For effective state secret supervision, this kind of legitimacy was inevitable, since these cases were often very delicate, involving actors in the political scene; if a Commissioner was elected with a consensus, he at least had the chance to maintain the image of an independent professional, and to distance the case from the political playfield, transforming it into a legal conflict.

However, some aspects of independence were not regulated adequately by the relevant acts. The office of the Parliamentary Commissioner for Data Protection and Freedom of Information was not a legal entity, but was a part of the Parliamentary Commissioners' Office, serving the other three parliamentary commissioners (the commissioner for human rights, the commissioner for national minorities, and the commissioner for future generations) as well. Since not the independent commissioners, but the Parliamentary Commissioners' Office had its budget set out in the respective act, the four commissioners had to agree on how to share this common budget; this situation was criticized by EU experts before the accession of Hungary to the EU, but was only changed with the setting up of the new authority in 2012.

18.2 A Plan for an Amendment: The Proposed Model of an "Information Commissioner"

After the 2010 elections, former opposition parties won a landslide victory: they obtained more than two thirds of the parliamentary seats. A massive reorganization of the state was about to begin; the government also indicated its plans to pass a new constitution. In this situation, I came up with my own plans regarding a reform of the Hungarian Parliamentary Commissioner for Data Protection and Freedom of Information. I proposed the model of an "Information Commissioner", first in a law journal, then as an official proposal sent to the parliamentary committee responsible for drafting the new constitution.[3] The committee's mandate, however, was terminated later on and the final text of the new "Basic Law" was drafted by a three-member committee set up by the governing parties.

With my proposal I had several goals in mind. The first was in line with my agenda aiming to build a new balance in information rights: data protection in Hungary had traditionally enjoyed a dominant role, and was often perceived by the

[3] http://www.parlament.hu/biz/aeb/info/adatvedelmi_biztos.pdf [in Hungarian].

public and the media as an obstacle in the way of transparency. Corrupt politicians quoted data protection law, when turning down FOI requests from journalists. One of my predecessors awkwardly called investigative journalism "nonexistent" because it is not in line with data protection; and this bad image of data protection law harmed the institution as well. From early on, I tried to promote FOI legislation, and when solving individual cases, I always tried to interpret data protection law to serve its original purpose, i.e. to protect the privacy of citizens, but in a way that is compatible with the interests of transparency and principles behind freedom of information. This is the reason, why I proposed a new, shorter title for the institution: "Information Commissioner" instead of "Parliamentary Commissioner for Data Protection and Freedom of Information", often abbreviated as "data protection commissioner". This new name would reflect that the institution is responsible for both areas, making freedom of information a key issue. The proposed new name for institution is not unknown at the international stage: similar bodies of the UK, Canada, or Slovenia carry the same or comparable titles.

Otherwise, the competencies and powers of the institution would have remained the same. It would have been (1) a fierce civil right advocate, with all the powers the Commissioner had had; (2) a quasi-ombudsman, with ombudsman-like powers and competencies; and (3) an enforcer of data protection and freedom of information. I proposed the new body to be given the power to impose fines, and, possibly, more administrative powers in the field of freedom of information, e.g., the authority to issue binding decisions on information qualifying as public data or not.

My proposal also included that the Commissioner should be provided with a separate office and budget (that is, to be planned by her/himself, and submitted directly to the Parliament), thus ensuring real organizational and financial independence. The rules of the election of the commissioner would have remained the same, maintaining the high level of political and professional independence the institution already enjoyed. Hence, after the proposed amendments, the situation of the Commissioner in terms of its independence and efficient functioning would have been improved. After the proposed amendments, Hungary would have had a general human rights ombudsman institution as well as an independent data protection/information commissioner responsible to the Parliament (such as Poland or Slovenia).

18.3 Context: High-Profile Data Protection Cases in 2010–2011

In 2010, the municipality of a small Hungarian town published a list of those who applied for social welfare but did not make use of it; thus, allegedly, harming the interests of the citizens of the town (the "shame-list"-case). The data controller in this case was a town, in which the mayor was the parliamentary leader of the governing party at the national level, one of the most influential government politicians. The plan was to shame those citizens who applied for benefits without a reason. But the list also contained personal data of those who could not make use of social welfare benefits because they died after they applied. Using my regulatory powers to protect innocent citizens from being exposed in public, I banned the publication

of this list. The municipality challenged my decision in court, which, however, found that the banning was in accordance with the law. The town assembly, then, passed a local decree making these data public. Since the decree was unconstitutional, I challenged it in Constitutional Court, which held the decree unconstitutional, and annulled it on 28 December 2011 – a accomplishment achieved on one of my last days in office.

I also used my administrative powers when I ordered the deletion of personal data relating to a government project called "Social Consultation". In this case, personalized forms were sent out to millions of citizens who should answer questions on government policies. The form included not only the name and address of the citizens, but also different bar codes. According to the legal assessment of my office, the project was neglecting applicable laws on processing personal data in the context of public opinion research. Most importantly, the consent clause on the form was illegal, since the necessary information to allow data subjects to understand what the consent to was not provided. If interpreted a certain way, the clause would mean that political views of millions of citizens could be processed by a government agency without any data protection safeguard. The agency in charge challenged my decision in court. The first court hearing was scheduled to be held on 20th February 2012.

Since my mandate was terminated on 31th December 2011, the new data protection authority carried on with the case as defendant; the plaintiff in the process is the agency in charge of the "Social Consultation" project, supervised by the government. The new data protection agency assigned a new lawyer for its representation in court. As the press reported,[4] the new lawyer had his offices "in the same building in the 1st district, on the same floor, and behind the same door" as the lawyer of the opposing party, i.e. the data controller. The lawyers of the two parties jointly initiated the delay of the first hearing; meanwhile, an officer of the newly set up data protection authority told the press that the new authority is to determine its "own position" in the case.[5] Since an act by the Government influences the outcome of an ongoing investigation, this situation, in my view, clearly demonstrates that the independence of the Hungarian data protection authority was breached (see below about the notion of "independence" as interpreted in the jurisdiction of the European Court of Justice).

18.4 Context II: Constitutional Changes in Hungary, 2010–2011

Much has been written about the recent political developments in Hungary after the 2010 elections; here I will mention only a few examples in order to shed some light on the change in the Hungarian system of data protection supervision. In Hungary,

[4] http://index.hu/belfold/2012/02/15/peterfalvi_megmentene_a_szocialis_konzultacio_kerdoiveit/ [in Hungarian].

[5] http://nol.hu/belfold/halasztast_kert_az_adatvedelmi_hatosag_a_nemzeti_konzultacio_miatt_inditott_perben [in Hungarian].

the assurance of independence for the most important constitutional institutions had been traditionally the need for a consensus between most of the political parties. For instance, the Chief Justice of the Supreme Court, constitutional court judges or the Ombudsman for Human Rights, as well as the Parliamentary Commissioner for Data Protection and Freedom of Information, were all elected by a two-thirds majority.

However, in the 2010 elections, governing parties acquired more than 2/3 of the seats in parliament. This was the end of the need for a consensus in parliamentary law-making regarding fundamental rights and the set up of important institutions. For instance, the way constitutional court judges are elected was changed; now the governing parties alone can nominate and elect judges. Following this legal reform, an MP and a former minister of the governing party was elected as a constitutional court judge. Furthermore, an independent Budget Council, whose members were normally elected by the Parliament, was scrapped, and a new one was set up. The Supreme Court was renamed to "Curia", and the mandate of the Chief Justice, a former judge of the European Court of Human Rights, was terminated prematurely on the last day of 2011, years before his term was originally supposed to end. One notable exception is the governor of the Central Bank: in fact, he could not be dismissed because of EU rules protecting the independence of national central banks.

18.5 Status quo: "National Agency for Data Protection and Freedom of Information"

Required by the EU Data Protection Directive, a consultative bill was sent to me that was setting out to abolish my office and substituting it by a new data protection office. Although this was no serious consultation process since I was given a 1-day period to give my opinion, I decided to not give in on that issue. Together with my colleagues, we wrote an opinion outlining 41 problematic points of the bill. Some of these points, mostly relating to technical questions, were accepted.

Apart from this incident, the new data protection act, in my opinion, can be viewed as several steps back in the field of both data protection and freedom of information. To quote some examples, the provisions relating to the scope of the act remain as they were, not in full compliance the EU Data Protection Directive. (This has serious consequences, since according to these provisions, the Hungarian act shall be applied to certain data processing operations that would be under other jurisdictions according the Directive.) Moreover, notification requirements will be more burdensome then they were before, which clearly goes against the development of data protection legislation in European Union, especially in the light of the draft Regulation. Binding corporate rules, which were burdensome to use even under the previous act, now cannot be used in Hungary as legal basis for data transfers to third countries. The so-called "new" act reflects an antiquated view on today's computing and data protection. In fact, the only major new element of the Act is the new data protection authority.

The new Data Protection Agency was set up on the 1st of January, 2012. It still has the same functions as the Parliamentary Commissioner for Data Protection and Freedom of Information had, although some powers were weakened, while some where somewhat strengthened. (1) The Agency might not have the adequate means, when it comes to act like a civil rights advocate; it now lacks many effective tools (for instance, it has no possibility to challenge acts in the Constitutional Court, its powers relating to state secret supervision were weakened). (2) The Agency still has an "ombudsman-like" function, straightforward procedures to deal with ordinary cases; and, (3), as an enforcer, the Agency can now impose (relatively modest) fines (up to 35,000 Euros).[6]

As to the independence of the new DPA: the head of the Agency was nominated by the Prime Minister, and he was appointed by the President of the State (who was also elected by the current governing party alone) on the 1st of January, for 9 years. My mandate was terminated on the same day by an Act with constitutional force, i.e. an act that cannot be challenged in the Constitutional Court of Hungary.

The new act does not regulate legal succession between the former Commissioner and the new Agency; there is only a provision authorizing the new Agency to investigate the ongoing cases started by the Commissioner. In practice, that meant that my former employees remained employees of the Parliamentary Commissioners' Office, and were all dismissed by their employer on the first working day of 2012. Some of them were re-hired by the new Agency; others were not. This process was clearly a violation of Hungarian employment law, and several former colleagues of mine initiated legal procedures.

The new Agency reports to the Parliament, and it now qualifies as a separate legal entity and has its own budget – these provisions can be regarded as steps in the right direction. There is, however, an odd rule in the new act regarding the declaration of financial assets: the Prime Minister can carry out proceedings to scrutinize the financial declaration of the head of the Agency, that can lead to his/her dismissal. This is a highly problematic point, and was raised by the European Commission when it started an infringement procedure against Hungary on this issue. Nonetheless, this is a point that can be changed relatively easily; one could have the impression that this is an intentional measure so that the Government can show the European Commission its willingness to change the Act in some points.[7]

18.6 Infringement Action Against Hungary

On 3rd October, 2011, three Hungarian NGOs, the Eötvös Károly Policy Institute, the Hungarian Civil Liberties Union and the Hungarian Helsinki Committee, in a letter to European Commission President Barroso asked for an investigation of the

[6] In my comments on the draft, I proposed a maximum fine of 350,000 Euros. However, my proposal was not accepted.

[7] Indeed, on the 2nd April 2012 the Parliament passed an amendment of the new data protection act, addressing the issue of the financial statement described above.

case concerning the "reorganization" of the Hungarian data protection authority, and initiated an infringement action against Hungary.[8] In their letter, they quote the seminal ruling of European Court of Justice (ECJ) from 2010 in the case of the European Commission v Federal Republic of Germany:

> independence of national supervisory bodies »precludes not only any influence exercised by the supervised bodies, but also any directions or *any other external influence, whether direct or indirect* [emphasis added], which could call into question the performance by those authorities of their task consisting of establishing a fair balance between the protection of the right to private life and the free movement of personal data.

According to the NGOs, "such a broad understanding of the independence of national data protection authorities does not only exclude direct state scrutiny over the national supervisory authority, as was the case in European Commission v. Federal Republic of Germany. Rather, it prevents member states from any sort of external influence, should it be direct or indirect." Therefore, independence also covers the protection from early, unfounded dismissal from office; the NGOs illustrate this point by analyzing the appointment and dismissal procedures of the members of the European Court of Justice, the members of the European Commission, governors of national central banks, and the European Data Protection Supervisor in this regard. The final conclusion of the letter sent by the NGOs is the following:

> national implementation of the Directive must, accordingly, make sure that the term of office of a person acting as the supervisory authority in the sense of Article 28 of the Directive is not removed from his office unless the preconditions usually relevant for the removal in the case of other independent institutions are met. This requirement is applicable irrespective of the level of the national law leading to the removal from office. Should it be otherwise, an important guarantee of EU law could be overridden by the member states and thus the supremacy of EU law would be challenged.

The letter was answered by Commissioner Reding on 30th November, 2011, who "ha[s] instructed [her] services to investigate [the] complaint and analyse the new [Hungarian] Act on informational self-determination and freedom of information which will repeal the current data protection legislation as of January 2012."[9] On December 12th 2011, Commissioner Reding requested information from the Hungarian government about, *inter alia*, the status of data protection supervision. The Commission touched upon the issue of premature dismissal by asking:

> "Why was it decided to replace the current supervisory authority with a new one? What are the reasons for not providing any interim measures until the term of the current data protection supervisor is due to end in 2014? How is it ensured that early ending of the Data Protection Commissioner's Office does not put in question the independence of the data protection authority as provided in EU law?"

The Commission also requested information about the conditions concerning the dismissal of the head of the new Agency.[10]

---

[8] http://www.ekint.org/ekint_files/File/barroso_dpa_independence_20111106_printed.pdf

[9] http://www.ekint.org/ekint_files/File/levelezes/response_laszlo_majtenyi.pdf

[10] http://www.kormany.hu/download/4/8b/60000/Letter%20from%20Vice-President%20Viviane%20Reding%20to%20Vice-Prime%20Minister%20Tibor%20Navracsics.pdf

According to the answer of the Hungarian Government (sent by the Deputy Prime Minister on 16th December 2011), the main reason for establishing the new National Agency for Data Protection and Freedom of Information was that the "ombudsman was not vested with enough power to remedy infringements."[11] The Government quotes my statement published in a press interview on 9th July 2011, saying that I'm not willing to continue as head of the new Agency. What is left out of the governmental response to the Commission is that I heavily criticized the "reorganization" of the Hungarian DPA as a breach of its independence. That way the government did not respect my mandate and "I would not, by any chance, fill any position nominated for by the Prime Minister without an election by the Parliament."[12]

It is also important to note that I was never approached by the Government, except for the mentioned draft act sent to me with a 1-day deadline to comment on it. In my response I detailed my position: setting up the new DPA infringes upon the EU Data Protection Directive. What should be furthermore told here is that the Deputy Prime Minister was accusing me in a speech to the Parliament of being motivated by personal interests rather than professional decency in the before-discussed "Social Consultation" case.

This incident, and other similar statements by leading government politicians could reasonably be interpreted as an informal way to exert pressure. The government's intention to remove me from office was clearly communicated; and in my opinion, already the uncertainty resulting from such a situation would amount to a breach of independence.

The three civil liberties organizations that submitted the first letter to the Commission also sent their answers to the questions of the Commission, illustrating their view on the current data protection supervision, and criticizing the government position.[13]

On 17th January 2012, the European Commission launched an accelerated infringement proceedings against Hungary.[14] There is no published information available about the communications between the Commission and the Hungarian government in the course of the infringement procedure. According to communications by the government addressed to the Hungarian public, the conflict can be easily resolved since the government is willing to amend the act responsible for the legal status of the new DPA.[15] The key question here is whether the premature termination of a mandate of the head of the DPA might qualify as breach of independence according to the Directive, or not; and if yes, what could be the means to remedy the situation.

---

[11] http://www.kormany.hu/download/1/8b/60000/Annex%20to%20the%20letter%20of%20DPM%20Navracsics.pdf

[12] http://www.origo.hu/itthon/20110708-interju-jori-andras-adatvedelmi-biztossal.html. [in Hungarian].

[13] http://tasz.hu/files/tasz/imce/letter_to_viviane_reding_29_12_11.pdf

[14] http://europa.eu/rapid/pressReleasesAction.do?reference=IP/12/24

[15] Ironically, this could mean that the Agency set up contrary to EU law would be even strengthened as a result of EU intervention.

In my view, the following measures might help to resolve the situation with the least possible adverse affects. In that sense, the Parliament should pass an Act that:

1. Qualifies the termination of the mandate as invalid, and reinstates the mandate until the original date, 29th September 2014; or the mandate is prolonged adding the interim period when I was deprived of office and therefore unable to fulfil my duties;
2. Shall change the name of the "National Agency for Data Protection and Freedom of Information" to "Office of the Parliamentary Commissioner for Data Protection and Freedom of Information";
3. Sets out that employees of the Office of the Parliamentary Commissioner for Data Protection and Freedom of Information enjoy the same privileges, i.e. the same legal status and allowances, as any other staff of the Parliamentary Commissioner for Human Rights, or of the former Parliamentary Commissioner's Office[16];
4. Reintroduces the right of the Commissioner to challenge acts in Constitutional Court;
5. Determines that the Office of the Parliamentary Commissioner for Data Protection and Freedom of Information is a legal successor of the former bureau of the Parliamentary Commissioner for Data Protection and Freedom of Information, and that the civil servants employed by the Commissioner until 31st December 2011 are to be further employed by the Office of the Parliamentary Commissioner for Data Protection and Freedom of Information;
6. Sets out, that the new obligation by the Commissioner to declare financial assets shall be suspended; the rules for the declaration of financial assets by the Ombudsman for Human Rights shall be applied for the Commissioner.

Although the infringement action is under way, the results are yet to be seen.[17] Article 47 and 48 of the draft Data Protection Regulation sets out in detail the requirements regarding the independent status of DPAs, among them those concerning personal independence. The Regulation determines the cases when duties of a member of a DPA may end ("in the event of the expiry of the term of office, resignation or compulsory retirement"), and sets out that "a member may be dismissed or deprived of the right to a pension or other benefits in its stead by the competent national court, if the member no longer fulfils the conditions required for the performance of the duties or is guilty of serious misconduct". While regulating the guarantees against unjustified premature dismissal in an EU legislative act that is directly applicable in member states is certainly a step forward, an even more detailed regulation might be needed to defend the independence of DPAs against "reorganization" plans of creative governments.

[16] The reason for this is that wages of civil servants of the "National Authority" have been reduced significantly in comparison with the staff of the Parliamentary Commissioner for Human Rights.

[17] On 7th March 2012, the infringement procedure entered into its second stage, as the Commission sent its reasoned opinion to the Hungarian Government (see http://europa.eu/rapid/pressReleasesAction.do?reference=MEMO/12/165&format=HTML&aged=0&language=EN&guiLanguage=en). On 30th March 2012, the Hungarian Government answered the reasoned opinion (http://index.hu/belfold/2012/03/30/ismet_valaszolt_a_kormany_brusszelnek/) [in Hungarian]; the letter of the Government is not yet public.

References

Colin J Bennett. 2002. The data protection authority: Regulator, ombudsman, educator or campaigner?. International Conference of Data Protection Commissioners, Cardiff, September 9–11, 2002. http://web.uvic.ca:8080/polisci/bennett/pdf/cardiff.pdf

Greenleaf, G. 2012. Independence of data privacy authorities (Part I): International standards. *Computer, Law and Security* 28: 3–13.

Schütz, P. 2012. Data protection authorities as a new regulatory approach. In *European data protection: In good health?* ed. S. Gutwirth et al., 125–142. Dordrecht: Springer.

Chapter 19
Data Protection, Social Networks and Online Mass Media

Artemi Rallo and Ricard Martínez

19.1 The Change in Public Communication Paradigm in the Information Society

At the dawn of the twenty-first century and in barely two decades, public communication has undergone a transformation, making the master picture we have always identified with unrecognisable. Communication based first on printing information and, later, broadcasting it audiovisually, corresponded to an information paradigm in which, firstly, the recipient of the information was a passive subject and, secondly, there were rules of time and space organising the reception of the object of public interest.

For centuries – and even until just a few decades ago – public communication was carried on almost exclusively through the exercise of the activity of providing information (whether or not this was journalism) and, consequently, the leading function in the democratic system of contributing towards forming public opinion was recognised only in the professionalised information provider. There was a *de facto* monopoly in communication in the hands of information providers defined by the scarcity of financial and technical means and by the characterisation of a professional activity, covered with singular legal guarantees intended to preserve the information provider's freedom for the sake of truth in information. Otherwise, information providers organised and ordered their information products over time (with a frequency in terms of hours, days or weeks, depending on whether it was a

A. Rallo (✉)
Consitutional Law, University Jaume I at Castellón,
Campus Riu Sec, 12080 Castellón, Spain
e-mail: rallo@uji.es

R. Martínez
Constitutional Law, University of Valencia,
13, Blasco Ibáñez Avenue, 46010 Valencia, Spain
e-mail: ricard.martinez@uv.es

S. Gutwirth et al. (eds.), *European Data Protection: Coming of Age*,
DOI 10.1007/978-94-007-5170-5_19,

printed or audiovisual medium); in space (with a territorial scope rarely exceeding the local or national sphere and, to increase its range, resorting to "correspondents"), and in the way the safeguards on their freedom allowed them to carry on without being conditioned by the subjects of the information or the recipients. Hardly any of the above was contradicted by the marginal possibility that a reader could write a "letter to the editor" of the printed media, or that newsworthy personalities could express their opinion or disagreement, or correct the content of information. Ultimately, media and journalists formed the monopolistic core on which a *passive communication model* constructed the formation of public opinion.

However, in a very few years, public communication has seen a transformation that compels us to speak of a certain change in paradigm in information methods. In the information and communication society structured around the Internet, the monopolistic position of the mass media and its professionals has given way to a plural, integrated model of communication sources in which bipolarity between the active subject of the information (mass media) and the passive receiving subject of the information (the public: readers, radio listeners and television viewers) has been done away with. Today, public communication witnesses an explosion of sources characterised by the fact that *primary communication sources* not only lie in professionalised journalistic media but instead are fed by a vast array of information tools that may or may not be professionalised (blogs, websites, audiovisual platforms, and social networks) which enrich, complete and help to construct the free flow of information. And, together with all of this, each member of the public acquires at least the character of secondary communication source, enjoying the tremendous opportunity to increase the wealth of information through comments, data and opinions that accompany the information flowing over the Internet almost without limit.[1] So, we can speak of *pluralistically integrated communication*, in which citizens leave behind their passive position, coming to occupy an unequivocally *active position* in public communication.

[1] All data point to a change in the way of access to traditional media. In Spain, AIMC (Asociación para la Investigación de Medios de Comunicación), in the report "Navegantes en la RED" (February 2012) states that a 51.3% of people read traditional and online newspapers, a 32% only read the online edition and a 9.3% only the printed version. In addition, a 68.4% are users of social networks of 68.4%, and a 67.1%. has read a blog in the last month. http://download.aimc.es/aimc/f5g9/macro2011.pdf (Av. 26/03/2012).

These data about social networks are confirmed in the Social Networks Observatory Report of The Cocktail Consultant that indicates the existence of a 85% of social network users (78% on Facebook). http://www.tcanalysis.com/2011/02/22/publicamos-la-3%C2%AA-ola-del-observatorio-de-redes-sociales/ (Av. 26/03/2012).

According to the report on the Use of Internet in Europe (comScore November 2011) a 47.8% of Europeans visit newspaper sites. A 12% come from Google, and a 10% from Facebook. This highlights the relevance acquired by social networks as a means of interaction with the readers of the media. http://www.comscore.com/esl/layout/set/popup/Press_Events/Press_Releases/2012/1/Nearly_50_Percent_of_Internet_Users_in_Europe_Visit_Newspaper_Sites (Av. 26/03/2012).

Moreover in Spain AIMC in the study "**La Prensa: digital vs papel**" (October 2011), highlights a continued access to traditional media accompanied by an increase in visits to online media (59% last month under the study). http://www.aimc.es/-La-Prensa-Digital-vs-Papel-.html (Av. 26/03/2012).

But a second element defines the current paradigm of free communication: *immediacy.* Today, communication has knocked down the walls of time and space to become communication in "real time". "There's nothing older than yesterday's paper" was the maxim proclaimed by news professionals for centuries to reaffirm the intrinsic link between information and the here and now, so that any *news item* told "today" mercilessly replaced "yesterday's" stories. In the time of the Internet, online news items immediately make "today's" edition of any printed medium old news. The "headline news" or "news flash" of any audiovisual communications medium now no longer enjoys such interest or attention, as it has been entirely replaced by the capacity of any member of the public to get news in real time.

Today, public communication is plural, integrated, active and immediate, and this is because the plurality of Internet services has transformed the paradigm of the public opinion formation process in the modern democratic society.

19.2 Social Networks and Online Mass Media[2]

Social networks undoubtedly constitute the main exponent of the transformation of communication in the contemporary world. Hundreds of millions of users of a single Internet portal (Facebook, for example) enjoy the extraordinary capacity to relate and communicate with one another: no mass media (not even the most world-wide audiovisual ones) ever dreamed of being able to reach such a potential audience.[3] And social networks undoubtedly constitute the biggest new feature of the past decade for the mass media, as they provide *interactivity* unprecedented until very recently. Today, almost all mass media have thrown themselves into social networks, whether as corporations or with the aim of opening up their most important programmes to interaction with users. In addition, mass media sporadically make use of content available on certain digital platforms (for example, videos) and open up many online news items to apparently anonymous comments or documentation from Internet users. It is common for the media to offer chats with people of public interest during which, in the style of a digital interview, Internet users fire questions which the interviewee answers in real or delayed time. This constitutes a journalistic format absolutely unthinkable just a few years ago. Television or radio stations commonly reserve spaces in their schedules in which they reproduce live the comments, information or questions from Internet users via the social networks into

[2] This article owes a great deal to the previous collective monographic work coordinated by Artemi Rallo and Ricard Martínez, *Derecho y redes sociales*. Pamplona: Civitas-Thomson Reuters, 2010.

[3] We will consider Social Networks from a legal approach as they have been defined by Article 29 Working Party:

"SNS can broadly be defined as online communication platforms which enable individuals to join or create networks of like-minded users. In the legal sense, social networks are information society services, as defined in Article 1 paragraph 2 of Directive 98/34/EC as amended by Directive 98/48/EC."

Article 29 Working Party. Opinion 5/2009 on social networks. (01189/09/ES WP 163). http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2009/wp163_es.pdf (Av. 31/03/2010).

which the media are integrated. Ultimately, the Internet user – the citizen – becomes an active subject in the production of news.

This foray by the media into the social networks brings positive consequences for them, but also risks, which should certainly not be dismissed regarding legal compliance. Security and trust.[4]

For mass media, the opportunity to open the way for members of the public who want to take an active part in the communication process is an inestimably valuable option. The chances for followers of online media to take a leading role are multiplying, and they range from conversation in real time to provocation.[5] Interaction in the social network allows the online medium to integrate users into the dynamics of programmes, secure their loyalty, take the pulse of opinion in real time and, given the capillary nature of these media, multiply the impact of each broadcast.[6] The more interactive followers a medium's digital platform has, the greater the *economic value* of the medium's communication offer: (a) higher volume and price of advertising inserted (b) and, most importantly, a greater chance of increasing the added value of the advertising offer on the communications medium. Behavioural advertising (based on the Internet user's history of accessing the online medium) takes on greater economic value than mere passive advertising. Ultimately, information value and economic value are blending in a scenario where the digital market is being transformed in a way that is as far-reaching as any offered in contemporary life.

To the phenomenon of social networks must be added the impact of the so-called blogosphere – which, in fact, came first in time.[7] What has come to be called

---

[4] It is interesting to at least show the point to which privacy-related problems are shared by authors on both sides of the Atlantic. Along these lines, Palfreman points out: "There are a series of environmental, financial, security, legal and privacy problems that will need to be resolved along the way (…)". **Security**: Servers holding such data could experience power outages or get attacked by hackers. Or the cloud provider could go bankrupt. Already there have been a few embarrassing incidents: Google Docs users were shut out of their online word processor documents for about an hour on July 8, 2008, and Amazon customers (including The New York Times) lost access to data for a few hours on July 20, 2008 following a power outage (…) **Privacy:** Lawyers have also raised the possibility that if an organization, such as a newspaper or university, stores its records online on a third party's server (e-mails, for example) those documents might not have the same Fourth Amendment protections from unreasonable government search and seizure as data stored on a personal computer». Jon Palfreman. "Dealing With Disruption. As digital media gets 'better, faster and cheaper. … [there is] little time for long-established human institutions like journalism to adapt" in *Let's Talk: Journalism and Social Media. Niemans Reports 63.3*, 2009, 19 accessed February 19, 2012, http://www.nieman.harvard.edu/assets/pdf/Nieman%20Reports/backissues/Fall2009.pdf

[5] It is not unusual, for example, in audiovisual media, for presenters to chat to viewers or to promise to carry out certain actions if they achieve a significant number of followers on one of the main social networks, such as Facebook.

[6] José Luis Requejo Alemán and Susana Herrera Damas. "¿Cómo crear comunidad a través de Twitter?: Nueve buenas prácticas en medios españoles*", La transformación del espacio mediático*, 3rd International Congress on Cyberjournalism and the Web 2.0, (Bilbao: Universidad del País Vasco, 2011), 666–681.

[7] José M. Cerezo, *La blogosfera hispana: pioneros de la cultura digital. Madrid:* Library of the Fundación France Telecom España, 2006. http://www.fundacionorange.es/fundacionorange/analisisprospectiva.html (Av. 19/03/2010).

citizen journalism. In general terms, citizen journalism constitutes an innovative explosion of social creativity going alongside the unprecedented expansion of the communication society sustained by the Internet. Every Internet user is a potential communicator contributing, with all the qualifications that should be made, to promoting true *democratisation of communication*. Providing information is no longer the prerogative of a particular professional sector as it was in other times. Instead, ownership of the right to inform has, in the digital age, taken on a universal meaning. Regardless of the use that can be made of this right and the judgment merited by the "excesses" covered by the exercise of it, there is no doubt that it is a phenomenon that contributes to expanding the freedom of individuals and incrementing democratic values. It is also an unstoppable phenomenon, as is the dizzying development led by the digital world in this knowledge age.

All this, however, does not mean that the scope and correct meaning of words do not require qualification. Citizen journalism expresses the universal potential of all individuals to contribute to communication in contemporary society, but it cannot either be classified as "journalistic activity" or considered to be deserving of all the legal and constitutional guarantees which contemporary democracies bestow on the right of news professionals to inform. While the latter deserve extreme constitutional protection when they inform truthfully about matters in the public interest, in accordance with a specific code of ethics, in order to preserve the free formation of public opinion, the product of the activity of the "citizen journalist" neither corresponds to the ethical code we have referred to nor, often, does it meet the requirements for truthfulness and public interest or specifically cover newsworthy "events". Instead, more often than not, it is a mixture of information, opinion, criticism, rumour, humour etc. And none of these has begun to earn it consideration and respect for contributing, as a new manifestation of individuals' democratic rights, to free, creative communication between citizens.

19.3 Personal Data Protection on Social Networks

However, in the above context of a change in public communication paradigm, expansion of online media and interaction between these and the Internet social networks, many questions can be raised about conflicts with the effective guarantee of the right to personal data protection.[8] And, in particular, from a legal point of view there are two main questions which must be raised: what are the regulatory requirements imposed on communication firms that have decided to move into social networks essentially covering the fundamental right to data protection? And, secondly, how will conflicts arising from the publication of information and opinion by users themselves develop?

[8] Artemi Rallo, "Protecting privacy in a fast, evolving more complex digital world", *Trends in global Communications: riding the next digital wave* (Barcelona: International Institute of Communications, 2010), 1–10.

For the application of personal data protection rules to social networks, a clear understanding of this singular context is essential. As Castells pointed out,[9] the development of the Net encourages the generation of communities through the transfer to the virtual world of pre-existing social groups and the creation of global interest groups. The Web 2.0 means the birth of a network society social universe with communities that can range from very local to any kind of horizontal grouping (professional or social groups); vertical grouping (spaces for group work); and even "informal" groups without limits of space or time. In addition, a large part of the services linked to it are leisure orientated and promote aspects directly related to personal or private life, such as sharing photographs, listening to music or sharing videos, or expressing opinion in the form of short 140-character messages. To this must be added a set of technical elements whose future influence is still unpredictable at the moment.[10]

Meanwhile, and also from the technological point of view, the web universe ceases to be a passive place and becomes a very dynamic social space. Users can express their opinions, obtain opinions from third parties, or show themselves. It is a complex environment where the applications do not always come from the principal provider[11] and users can, at the same time, be beta-testers and developers.

The Web 2.0 therefore goes much further. It is not just a set of software resources at different levels of advancement. It means the birth of a social universe belonging to the network society populated with communities that can range from the most local to any kind of horizontal grouping (professional or social groups); vertical grouping (spaces for group work); and even "informal" groups without limits of space or time.. Internet users are in a perfect position to turn all their concerns and needs into social communication. The basic circle of human and social relationships is expanding: there is no space or time limit conditioning its possibilities for communication with any imaginable environment. There is a *permanent invitation* to join communication spaces, to the degree or level of intensity the user wishes, in order to share manifestations of all kinds which can be employment-related, emotional,

[9] Castells points out very graphically: "The Internet is an extension of life as it is, in all its dimensions and forms. Moreover, even in roleplay games and informal chatrooms, it is real lives (including real online lives) that determine and define the online interaction model," Manuel Castells, *La galaxia Internet. Reflexiones sobre Internet, empresa y sociedad* (Barcelona: Areté, 2001), 139. To understand the capacity of networks to define community spaces, the chapter in this work devoted to virtual communities is particular interesting (137–158).

[10] Artemi Rallo, "Internet of the Things: the importance of privacy oriented strategies", *The 2nd Internet Annual of Things Europe*, Brussels, 2010, 1–8. See http://www.theinternetofthings.eu/

[11] In this respect, the findings of the Canadian Data Protection Commissioner in her investigations into Facebook are particularly important.

Elizabeth Denham, *Report of Findings into the Complaint Filed by the Canadian Internet Policy and Public Interest Clinic (CIPPIC) against Facebook Inc. under the Personal Information Protection and Electronic Documents Act. July 16, 2009*. Office of the Privacy Commissioner of Canada. PIPEDA Case Summary #2009-008. At http://www.priv.gc.ca/cf-dc/2009/2009_008_0716_e.cfm (Disp. 16/04/2010), pages 38 and 94.

informative, educational, etc. All individuals could become promoters/receivers of infinite impacts, faced with which, far from adopting a passive position, they want to act and add to the permanent offers they receive with others of their own.

19.3.1 Identity as the Keystone

The Web 2.0 is now not just the *information Internet,* if we characterise this as the mere factual transmission of a unique, qualified broadcaster to a huge, heterogeneous, diffuse mass of recipients. The Web 2.0 has mutated the technical and the human, it has inoculated human behaviour with technology and it has wired the *Internet of individuality*: each individual/user constitutes an active and passive pole, generating content.

But individuals can show themselves on the Internet in multiple forms. (1) Today it seems there is still a huge range on the Net so that users can still benefit from in a *passive* and apparently *anonymous* way from infinite information services that meet their costs with the ultimate result of projecting their content to the end recipient – the individual. This original expression of the Internet, with a limited relationship between the information and users hidden behind their computer screens, is still apparently widespread although, in practice, this is increasingly subverted by many linking, identification and Internet access traceability techniques. (2) The Internet is multiplying its individualised "paid-for" services in which the subject obtains satisfaction and response to an immediate, personal need (usually quantifiable or with an economic dimension) like those traditionally offered by the real market (renting a flat, buying a product, etc.). In this context, users appear as true holders of rights, obligations and even legal relationships constructed in the form of Law, which require, as an inexcusable *prius,* the ability to identify of anyone personally registering as a recipient or generator of these relationships. (3) But the most recent and advanced technological developments on the Internet are largely focused on an incontrovertible reality: in the modern information and communication society, the *currency* of payment for infinite services is – it seems unavoidably – *personal information*.[12]

As is well known, when browsing, Internet users leave a trail that obviously has an economic value; in other words, for providers of Internet services user browsing is economically very profitable. This economic profitability is no longer linked to the attitude of the Internet user as a passive recipient of advertising, which obviously continues to have an undeniable value that increases with greater volumes of access. Today, thanks to Internet operational routines and IP tracing, the basic information about the applications installed on our computers, cookies and browsing logs, user

[12] See Ignacio Alamillo Domingo, "La identidad electrónica en la red", *Derecho y redes sociales*, ed. Artemi Rallo and Ricard Martínez. (Pamplona: Civitas-Thomson Reuters, 2010) 37–53.

profiles are generated which can be used to establish general browsing profiles that acquire a multiplied market value.[13]

Following a browsing trail, even without specifically identifying the Internet user, provides extraordinarily valuable information if it is contextualised. Users unconsciously reveal all kinds of preferences, indicating the subjects that interest them, the graphics that attract them and the publications they prefer. These electronic footprints are used to make browsing easier and quicker, to present advertising in a certain way and carry out market studies, or to offer customers who have identified themselves personalised services adapted to their web browsing.

If, based on its basic and "traditional" operation, the Internet presented a challenge to the protection of private life, greater complexity lies in the social networks, where general user profiles and fictitious identities will no longer do. To be effective on a social network – to achieve their aims – individuals identify themselves. And, in this context, identity has an extraordinary value because, thanks to it, the information, the message or the advertising are personalised. There will be the capacity to establish or identify circles of trust[14] and, thanks to them, the viral nature of messages multiplies the efficiency and effectiveness of processing.

While on the traditional Net – largely a producer of content intended for passive users – the risk to the protection of privacy and personal data was significantly limited, on the Web 2.0 the conflict between the Internet and data protection appears impossible to resolve. While on the traditional Web in order to avoid risks to user privacy it was enough to be anonymous or to have a fictitious identity, on the interactive Web this response appears to be highly unrealistic in that the identification of the Internet user lies at the heart of the utility of a good part of its services. This is particularly the case with the social networks: minimising the risks for data protection and subscriber privacy in these services (restricting a good part of the personal information required in the form of photographs or sensitive information) runs up against an insurmountable limitation – the need for users seeking to relate to one another to identify themselves. All this makes it particularly necessary and imperative that the actions of Internet providers and users should be subject to rules aimed at protecting the personal data of individuals (active subjects of digital communication or any member of the public whose personal data is supplied over the Net, whether or not they are users).

Because of this, the answer to the first question we initially asked ourselves on whether there are principles applicable to the Internet and, in particular, to the social networks, the answer may be no other than yes. The heart of the question does not,

[13] See Paul M. Schwartz, "Internet privacy and the State", *Connecticut Law Review* 32 (2000) 815–859 and ee Article 29 Working Party. Opinion 2/2010 on online behavioural advertising. 00909/10/ES GT 171. Available at http://bit.ly/dsAN9F (Av. 26/03/2012).

[14] In fact, this is Google's most recent commitment with its Google+social network: "The first of the tools or services included is Circles, a tool allowing you to create circles of people whose members can debate, publish and share all kinds of information only with defined groups of contacts, such as family, schoolfriends, workmates, teammates, colleagues, etc." See http://www.puromarketing.com/16/10334/google-project-nueva-social-google-llega.html

therefore, lie so much in whether there are basic applicable principles, as these clearly exist, but rather in whether they are really taken into account in the initial design of applications.[15]

19.3.2 The Application of Personal Data Protection Rules to Social Networks

The processing of personal information constitutes the core element of social networks. This is the case both from the point of view of service providers, whose business is based precisely on the profits produced by exploiting this information, and that of users, who show their information and, with it, show themselves personally and professionally. The ultimate right in this context can, therefore, be none other than the right to data protection.

19.3.2.1 The "Lindqvist Case" as a Standard for the Applicability of Social Data Protection Rules to Social Networks

Without any manner of doubt, the *Bodil Lindqvist case* constitutes a most important reference when it comes to establishing criteria for applying data protection regulations to social networks.[16] In this case, the Court of Justice of the European Union clearly defined the criteria to be followed in personal data processing on a website.

It is important to bear in mind that behaviour consisting of publishing a photo, video or written text on a social network does not materially differ in any way from the Lindqvist case. We are looking at an identical situation, differing only through the fact that the technology has advanced, making it possible to act on the Internet without prior technical knowledge and in a cooperative environment.

In Lindqvist, the Court of Justice concluded that the conditions existed for the application of Directive 95/46/EC concerning personal data protection. These are:

---

[15] Along these lines, over the last few years more work has been done on Privacy Impact Assessment and Privacy by Design methodologies whose approach coincides with what has been pointed out here: the providers and programmers must take into account, *a priori*, in their design, methods ensuring respect for users' rights to private life. . See Lawrence Lessig. *Code version 2.0.* Basic Books. (New York: Perseus Books Group) 2006. Available at http://codev2.cc/download+remix/Lessig-Codev2.pdf

On this matter, there is increasingly abundant documentation, although the reference methodology is that of the British Information Commissioner's Office. ICO. *Privacy Impact Assessment (PIA) handbook (Version 2).* 2009. http://www.ico.gov.uk/upload/documents/pia_handbook_html_v2/index.html (Av. 22/03/2010).

[16] Decision of the Court of Justice dated 6 November 2003 on case C-101/01. Reference for a preliminary ruling raised by the Göta Hovrätt. http://curia.europa.eu/

1. *Existence of "processing" of personal data:*

> 27. The answer to the first question must therefore be that the act of referring, on an Internet page, to various persons and identifying them by name or by other means, for instance by giving their telephone number or information regarding their working conditions and hobbies, constitutes 'the processing of personal data wholly or partly by automatic means' within the meaning of Article 3(1) of Directive 95/46.

Because of this, the Court of Justice alluded to the circumstances/situations that must be included in the legal concept of processing which, it must be stressed, include the concept of "disclosure by transmission" and "dissemination" as concepts forming an integral part of the transfer of personal data.

> 25. According to the definition in Article 2(b) of Directive 95/46, the term 'processing' of such data used in Article 3(1) covers 'any operation or set of operations which is performed upon personal data, whether or not by automatic means'. That provision gives several examples of such operations, including disclosure by transmission, dissemination or otherwise making data available. It follows that the operation of loading personal data on an internet page must be considered to be such processing.

2. *Non-applicability of the private life exception.*

> 47. That exception must therefore be interpreted as relating only to activities which are carried out in the course of private or family life of individuals, which is clearly not the case with the processing of personal data consisting in publication on the internet so that those data are made accessible to an indefinite number of people.

3. *It is for the national authorities or judge to resolve the conflict between the rights to data protection, freedom of expression and information.*

> 90. The answer to the sixth question must therefore be that the provisions of Directive 95/46 do not, in themselves, bring about a restriction which conflicts with the general principles of freedom of expression or other freedoms and rights, which are applicable within the European Union and are enshrined inter alia in Article 10 of the ECHR. It is for the national authorities and courts responsible for applying the national legislation implementing Directive 95/46 to ensure a fair balance between the rights and interests in question, including the fundamental rights protected by the community legal order.

The Lindqvist Decision therefore unequivocally resolves any original question marks that might have existed over the validity and applicability of personal data protection rules on the Internet by extending the guarantee of such rights to all computerised processing operated on the Net. And, although the original case constitutes a paradigmatic example of the digital situation of the original Internet environment, where the creators of websites were the content generators (including personal information), its impact is substantially greater in the interactive situation under Web 2.0, where users as well as service providers have the unlimited opportunity to supply personal content subject to the same computerised processing. However, it is no less true that the relative initial ease in identifying positions and responsibilities on the Internet (those responsible for content versus passive users) is extraordinarily blurred on the Web 2.0, where both providers and users actively feed the content of Internet services.

If we apply the conclusions of the Lindqvist Sentence literally to an opinion on the "wall" of a social network, it is clear that, under certain conditions, there would be processing subject to the Directive pointed out by Article 29 Working Party. And the same would happen if a photograph was tagged or a video published concerning identified or identifiable people. In practice, as we will see below, the private life exception will only be applicable when the space on the social network is configured in such a way that it is visible only to an expressly authorised group of friends. Otherwise, the Lindqvist circumstances would fully occur.

19.3.2.2 Opinion 5/2009 of the Art. 29 Working Party on Social Networks

In Opinion 5/2009 concerning online social networks,[17] the Art. 29 Working Party establishes the conditions for the application of Directive 95/46/EC,[18] based on the consideration that in "a legal sense, social networks are services of the information society". Initially, it is clear that, for this kind of service to work, it is necessary to process personal data in a particularly important way through registration and setting up the user profile. Meanwhile, and considering that the ultimate aim of a social network is to interact with other users, each of them provides information – in the form of descriptions, opinions, photographs, etc. – and the social network provides them with tools – lists of users, private messaging, e-mail, etc. – that facilitate this and for which it is necessary to carry out some kind of processing.

From this point of view there is no doubt over the applicability of the European Data Protection Directive. From here, the Working Party focuses its effort on breaking down each of the elements present in such processing. Along these lines, there is one aspect where there is no room for doubt: "The provisions of the Data Protection Directive apply to SNS providers in most cases, even if their headquarters are located outside of the EEA."[19] However, the complexity of this type of services makes it necessary to set criteria identifying other possible responsibilities: these responsibilities will cover both external application providers when they process data and, under certain conditions, users themselves:

1. When the social network is used as a cooperation platform for an association or business.
2. And, secondly, when, in the understanding of the Working Party, social network users will assume responsibilities over the content generated in singular but very

[17] Article 29 Working Party. Opinion 5/2009 on social networks. (01189/09/ES WP 163). http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp163_en.pdf (Av. 31/03/2010).

[18] Directive 95/46/EC, dated 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

[19] The Working Party pointed out that there is processing which cannot be carried out without using the user's own computer, generally involving cookies, so resources in European territory would be used. See WP148, Opinion 1/2008 on data protection issues related to search engines.

common circumstances: "When access to profile information extends beyond self-selected contacts, such as when access to a profile is provided to all members within the SNS or the data is indexable by search engines, access goes beyond the personal or household sphere. Equally, if a user takes an informed decision to extend access beyond self-selected 'friends' data controller responsibilities come into force. Effectively, the same legal regime will then apply as when any person uses other technology platforms to publish personal data on the web."

3. Nor is user processing of third parties' personal data without their knowledge considered to be excluded from data protection regulations through the so-called *domestic exception,* and/or particularly when this concerns especially protected data.
4. Finally, the Working Party recalls that, in certain situations, the domestic exception will also not apply when rights such as freedom of expression, the right to information or the freedoms of artistic or literary creation prevail. In the same way, it also does not exclude the application of the general provisions of national civil or criminal law.

19.3.2.3 The Spanish Data Protection Agency and Social Networks

The Spanish Data Protection Authority has carried out various actions in this area, promoting and participating in studies,[20] issuing reports or resolving the protection of the right to data protection or the application of the legally established penalty system. Documents that contribute in some way to defining the institution's positions on this matter should be highlighted. In particular, the recommendations to Internet users published in 2009 are significantly indicative. This document notes an interesting change of point of view in which, whereas in previous editions the user had been conceived as a passive subject whose data was subject to processing, the current recommendations contained in points X and XI of the document point to a new approach. Firstly, the incontrovertible reality that regular and everyday use of Web 2.0 resources can determine the processing of data and images of people who have not authorised their use is taken as a starting point, and it is recommended that a special duty of care should exist.[21]

[20] Spanish Data Protection Agency. INTECO. *Estudio sobre la privacidad de los datos personales y la seguridad de la información en las redes sociales online*. Madrid, 2009 (english version available in http://www.inteco.es/file/vuiNP2GNuMjfCgs9ZBYoAQ).

[21] Three specific recommendations are orientated towards this:

"Take special care over publishing audiovisual and graphic content on your profiles, especially if you are going to host images relating to third parties.

- Do not label audiovisual content with the real identities of those appearing or offer data from third parties on your space without their consent.
- When you publish a photo or write a blog you may be including information about other people. Respect their rights".

Meanwhile, the document also takes into account other Internet users who consciously use Web 2.0 resources for information purposes. For this reason, the Recommendations are very specific and point unequivocally towards the need to raise user awareness of the conditions for exercising the right to information on the Internet.

Together with this promotional activity, the Spanish Data Protection Agency has adopted important legal decisions in that its reports and resolutions serve to guide operators' actions. So, for example, Report 615/2008[22] deals with the common, everyday practice of "individuals who use their websites to share photos of their children doing extra-curricular activities".

The report firstly analyses whether the conditions for the application of the domestic exception established in the European Data Protection Directive are met, concluding as follows: (1) Firstly, taking the Lindqvist Case as a reference, the exception would not apply because we are not in the sphere of the private or family life of the individuals when the publication of the information is projected beyond the domestic sphere. Which, with respect to pictures on the Internet, occurs when "there is no limit on access to them". (2) Secondly, taking the aforementioned Opinion 5/2009 of the European Group of Data Protection Authorities, concerning the identification of the indices pointing towards the existence of treatment subject to the Directive into account, the following conclusion is drawn:

"In order for the exclusion established in article 2 of the Data Protection Act to exist, the important thing is that it should be an activity involved in a personal or family relationship equivalent to one which might be carried out without use of the Internet. These circumstances would therefore not exist, as publication has been made on a site that is freely accessible to everyone or where the large number of people invited to contact the site indicates that such an activity extends beyond the circumstances of such a sphere."

In conclusion, the configuration of the website is very important for the purposes of determining the applicability of data protection legislation. Social network users take on a singular leading role in designing their position on the Web 2.0 and, consequently, generate the responsibilities inherent in the decisions deriving from their activity on the Net: unlimited access via search engines to content previously put in a user's account or profile transforms the nature of the communication maintained and bestows an obligation to act carefully and to protect others' rights.

Finally, reference must be made to various resolutions by the Spanish Agency made in the context of proceedings to impose penalties and/or protect rights affecting Web 2.0 services. Firstly, situations relating to Internet platforms hosting and unlimitedly disseminating audiovisual content have been raised. In this area, the Spanish Agency has based its resolutions on the doctrine of Opinion 4/2004, dated 11 February, of the Article 29 Working Party concerning personal data processing via videocamera surveillance: "the data consisting of image and sound are personal". The identifiable nature of such data "can result from the combination of the data

[22] See http://www.agpd.es/portalwebAGPD/canaldocumentacion/informes_juridicos/index-ides-idphp.php

with information from third parties or even from the application, in the individual case, of specific techniques or devices". Based on this premise, the Spanish Agency has concluded: "The capture and reproduction of images of passers-by in the street constituting personal data and its publication on YouTube, accessible to any Internet user, is subject to the consent of its owners, in accordance with the provision of article 6.1 of the Data Protection Act".[23]

This approach has been qualified and adapted to the reality of the Internet with a commitment to prioritising the exercise of the right of cancellation as a method for resolving conflicts, reserving the structure of penalties for the most important offences. So, the AEPD understands that the reality of the Internet requires an interpretation of the principle of consent adapted to the situation for which it is intended, where strict application would lead to paralysis or to the identification of a huge range of circumstances that could potentially be classified as breaches of the right to personal data protection for millions of people who are easily accessible using a mere search engine and for whom prior consent would be impossible. It follows that the principle that should be attended to is the one stating that, when the legal system offers various remedies, the exhaustion of formulas which, if possible, allow the cancellation of data and, an end to the processing of the personal data, is the most appropriate course. The AEPD has sought to obtain correction for breach of the regulations by upholding the right to cancel illegitimately used data. This premise has not, in certain circumstances – particularly when sensitive data or particularly seriously affected rights and the breach of professional secrecy are involved – prevented the activation of the legally established penalty mechanisms, following the doctrine issued by the Opinions of the Art. 29 Working Party.[24]

19.3.3 Personal Data Protection Policies Concerning Social Network Pages Managed by Online Mass Media

In view of the criteria sketched out by courts and personal data protection authorities, an initial conclusion appears to be clear: media opening up a space on Facebook will be obliged to comply with basic personal data protection regulations.

Having studied six of the principal Spanish mass media,[25] only one of them (the radio broadcasting network *Cadena SER*), has any kind of rules[26] for it users covering

[23] See PS/00479/2008, Available at http://www.agpd.es/portalwebAGPD/resoluciones/index-ides-idphp.php

[24] See PS/00508/2008.

[25] Cadena SER, Cadena COPE, Onda Cero, Televisión Española, Telecinco and La Sexta TV.

[26] http://es-es.facebook.com/cadenaser?sk=app_214923178538944

the impact of social networks on online mass media and the direct effect of data protection on users accessing it via this digital channel:

> Rules for participation.
>
> The purpose of the Facebook pages managed by Cadena SER is to establish a direct relationship between the radio station and its different programmes and their followers.
>
> To achieve this, the following participation rules are established, which are additional to the rules of Facebook. The latter can be consulted at http://www.facebook.com/terms.php?locale=ES:

- All opinions are welcome, but avoid insults and language that incites hate, discrimination, the promotion of illegal activities or that is racist, violent or xenophobic. Publish your opinion, but respect other users and Cadena SER.
- Write your comments only ones and avoid capital letters, which, on the Internet, are considered as shouting. Written abuse will be considered as spam.
- If a subject for debate is suggested, stick to it. The Internet has many other places where you can discuss anything you like.
- The Facebook pages managed by Cadena SER do not allow advertising by companies or for events of any kind or political propaganda. Nor do they allow the promotion of other Facebook groups or pages or other social networks not belonging to Cadena SER or other Prisa Group companies.
- Do not share copyright-protected content without the authorisation of the rights holder.
- Do not publish personal data, as it can be seen by all visitors.[27]
- The team administering the Facebook pages managed by Cadena SER reserves the right to delete any message or content that does not comply with these regulations or to block any user who repeatedly breaches them, and it accepts no responsibility for their breach or for the consequences that this may involve.

As can be seen, these are the usage policies of a forum, and only one of them makes a vague reference to personal data protection.

By contrast, if we consult the space of the Spanish Data Protection Agency[28] generated on Facebook alongside the organisation of the 31st International Conference of Data Protection Authorities in Madrid in 2009, we can read the following information: "By becoming a fan of this page you consent to: (1) the processing of your personal data in the Facebook environment in accordance with its http://www.facebook.com/policy.php?ref=pf privacy policies; (2) access by the AEPD to the data contained in the fan list; and (3) news items published about the event appearing on your wall. The AEPD will not use the data for other purposes or for sending additional information. If you no longer want to be a fan, all you need to do is to click on the link below on the right "Cease to be a fan". You may exercise the rights of access, correction, cancellation and challenge at any times by writing to Agencia Española de Protección de Datos, Secretaría General, C/Jorge Juan n 6, 28001 Madrid or by

[27] The underlining is the authors'.

[28] http://es-es.facebook.com/AEPD?sk=info

sending an e-mail to the address privacyconference2009@agpd.es, accompanied by a photocopy of an official document identifying you.. If the document is sent by e-mail, you must digitally sign the message or attach a scanned official document. Concerning this processing, you must bear in mind that the Spanish Data Protection Agency may only consult or remove your data as a fan. You must make any correction to it via your user configuration. E-mail address: ciudadano@agpd.es".

What is the reason for this significant difference? It is clear that, when a company acts in a social network, it is obliged to comply with the applicable legal provisions concerning data protection, as argued in the preceding pages.[29]

Various scenarios can be differentiated, but the most common one consists of the company registering as a user on the most commonly used spaces: that is, Facebook, Tuenti, Twitter and, sometimes, YouTube. In this case, it is a hybrid situation, as, in part the organisation will act like any other user of the social network while, on the other hand, it will also assume legal liabilities for the action it carries out. So, when a communication space is opened up on a social network, the organisation/institution/company/communications medium will act as what the Spanish Data Protection Agency and Spanish case law have defined as a personal data *controller*:

> As has already been stated, it can also be derived from the repeated sections of art. 3 that controllers are differentiated depending on whether decision-making power is exercised over the file or over the actual processing of the data. So the party responsible for the file is whoever decides to create the file and its application, content and use; that is, whoever has decision-making capacity over all the data recorded in that file. However, the responsible for processing is the subject to whom decisions on the actual processing activities for the data are attributed; that is, over a specific application. These would be all circumstances where decision-making power must be differentiated from actually carrying out the activity making up the processing."[30]

As a result of this Decision, art. 5 of Royal Decree 1720/2007, dated 21 December, approving the Regulation developing the Data Protection Act 15/1999, dated 13 December, defined the controller for the file and the controller for processing as follows:

> q. Controller for the file or for processing: Individual or public or private organisation or administrative body which, alone or together with others, decides on the purpose, content and use of the processing, even though it may not actually be carried out.
>
> Bodies without a legal identity acting in the process as differentiated subjects will also be controllers for the file or for processing.

The circumstances defined in the decision and in the previous precept therefore occur here: this is personal data processing in that a user opening an account lacks

[29] See Mónica Vilasau Solana. "Privacidad, redes sociales y el factor humano", in *Derecho y redes sociales*, ed. Artemi Rallo and Ricard Martínez. (Pamplona: Civitas-Thomson Reuters, 2010), 66–71.

[30] See the Decision dated 5 June 2004, of the Third Chamber for Contentious Administrative Proceedings of the Supreme Court concerning differentiation between the concept of the controller for the file and the controller for processing, confirming the decision of 16 October 2003 of the First Section of the Chamber for Contentious Administrative Proceedings of the National High Court, handed down in appeal number 1539/2001. Available at http://bit.ly/oDvST6

complete control over the ownership of the social network file. Because of this, the obligations deriving for the organisation/body concerning compliance with data protection legislation are limited and, in this way, for example, there will not be a duty to register a file or to conclude a contract for access to data on behalf of third parties.

It must be borne in mind, firstly, that the online communications medium is limited exclusively to registering with the social network and using the tools existing there, without enjoying any decision-making capacity on the structure, organisation or material management of the data other from that enjoyed by the social network itself. Its position cannot be identified with that of any other user of the social network, as the following conditions are not met:

1. Acting as a user interacting in the social network system.
2. Not incorporating personal data in its own resources.
3. Not contracting any service provision for developing or maintaining the space with the social network provider.
4. Not agreeing additional services with the provider, such as behaviour analysis, monitoring or drawing up user profiles, whether or not these are associated with the broadcast of behavioural advertising.[31]

In these circumstances, to ensure proper compliance with data protection legislation, the online mass media should proceed as follows.

Firstly, it should comply with the duty of information to users on the use of any personal information that may be supplied due to the existence of personal data processing and the enforceability of respect for principles and compliance with the obligations established in the current legislation. For this purpose it is recommended to: (1) place a brief piece of information in the space in the account provided by the social network giving basic information about the identity and location of the responsible party, the purpose sought and ways of exercising data protection rights; (2) develop a welcoming procedure for new friends with an e-mail that includes this information; (3) hyperlink to corporate privacy policies.

[31] Behavioural advertising is based on the continuing observation of the behaviour of individuals. It seeks to study the characteristics of such behaviour through their actions (repeated visits to a specific site, interactions, key words, production of online content, etc.) to develop a specific profile, thereby providing users with advertisements customised based on the interests inferred from their behaviour. Behavioural advertising normally involves the collection of IP addresses and the processing of unique identifiers (using cookies). The use of such devices makes it possible to isolate users without knowing their real names. In addition, the information collected refers to characteristics of behaviour of a person and is used to influence that specific person. This profile is accentuated when taking into account the possibility that profiles are linked at all times with directly identifiable information provided by users, such as the information provided on registration.It must be taken into account that a technologically available possibility is defined here. The decision on whether to use these techniques will correspond to editors, advertisers and advertising service providers.

See Article 29 Working Party. Opinion 2/2010 on online behavioural advertising. 00909/10/ES GT 171. Available at http://bit.ly/9hhMmK and Miquel Peguera Poch, "Publicidad online basada en comportamiento y protección de la privacidad", in *Derecho y redes sociales*, ed. Artemi Rallo and Ricard Martínez. (Pamplona: Civitas-Thomson Reuters, 2010), 354–380.

In addition, following the indications established in Opinion 5/2009 of the Art. 29 Working Group mentioned above, information should particularly be obtained on: (1) The use of data with direct sales purposes. (2) The possible distribution of data to specific categories of third parties. (3) The use of sensitive data. (4) Integration into the environment of third party applications capturing or processing data from "friends" when such integration depends on the wishes of the user responsible for the account.

Secondly, it must be pointed out that there can be no other reason legitimising the processing of personal data in these social network spaces managed by online communications media than the consent established in data protection legislation[32] – which will be understood to be granted when a request to "become a friend of" is made or when "an invitation is accepted". However, the following must also be taken into account:

1. such consent affects only the data of the person who is added, never third parties related to a "friend" whose profiles may be open;
2. the possible existence of exceptions to the rule of consent must be examined on a case-by-case basis strictly following the regulations;
3. an open profile "does not imply consent". It must be remembered that, as the Spanish Data Protection Agency points out in its Report 0342/2008, the Internet and, therefore, social networks, are not sources accessible to the public[33] and authorisation for the use of personal information without the prior consent of the owners of such data is not permitted.
4. The incorporation of data such as e-mail addresses into systems constitutes processing subject to data protection legislation and the fact that it is accessible in a social network environment does not necessarily provide justification legitimising processing.
5. The guarantee of "friends'" rights has limited content. It is governed by the rights of access, correction, cancellation and challenge to the processing. However, (a) the content of the right of access will be defined by the possibilities offered by the network and each specific user's capacity for access to profile information.

[32] See Mónica Arenas Ramiro. "El consentimiento en las redes sociales online", *Derecho y redes sociales*, ed. Artemi Rallo and Ricard Martínez. (Pamplona: Civitas-Thomson Reuters, 2010), 117–144.

[33] Recently the Spanish Supreme Court stated that the Section 10.2.b of the Spanish Data Protection Regulation must be abrogated because it contravenes the art. 7 of the Directive that regulates the legitimate interest. In any case those who process data from an open profile on a social network must prove this interest conceived as "Interest of a person recognized and protected by law" or "legal situation holds in relation to the actions of another person that involves the power to require, through an administrative or judicial proceeding, a behavior consistent with law."

See Ricard Martínez Martínez. "Interés legítimo y protección de datos personales en la sentencia de 8 de febrero de 2012 del TS" in El Derecho, http://www.elderecho.com/administrativo/Interes-proteccion-personales-Tribunal-Supremo_11_372805001.html (Av. 23/03/2012).

It will therefore, for practical purposes, be sufficient to offer screenshots showing the data accessed to anyone exercising the right. (b) The right to challenge, correction and cancellation will be modulated. The party responsible for processing must meet it concerning the aspects of the application under its control – such as, for example, modifying or deleting a commentary from the wall. The correction of aspects related to the user profile will normally be exercised before the provider. Erasure or blockage, when this consists of "ceasing to be friends", may be exercised by both parties.

6. There will be limits concerning the use of data. The principle of purpose constitutes an insurmountable limitation and will be bounded by the conditions of use of the social network, which may prohibit specific uses of the information available and actually provided "when making friends".
7. The controller mus comply the principles of security and secrecy, but they must be adapted to the conditions of the environment, affecting only the processing actually carried out.

19.4 Opinion, Information and Personal Data Provided by the Users of a Social Network in Online Mass Media: Legal Importance and Liability

To end the examination of the issues related to the use of social networks, it is appropriate to look at what is undoubtedly the essential objective of these spaces: encouraging users to freely show their opinions.

In principle, given the nature of the environment, we are considering mass media that fully exercise the freedoms of information guaranteed by the Constitutional Regulation, which means that a particular judgment must be made in clashes between this right to inform – and, basically, of the public to be informed – and any other fundamental right coming into conflict with it. In particular, the search for balance between the full exercise of freedoms of expression and information – indispensable in order to ensure the formation of truly free public opinion – and the right to the protection of privacy and personal data is singularly difficult in general and, in particular, when Internet social networks interact.

There is no room for doubt on the preference which will be given most of the time, in the analysis of this specific case, to the freedom of information against data protection when these come into conflict, and the high constitutional value of the democratic principle rooted into the free formation of public opinion when whoever is exercising the right to inform in mass media. However, an improper use of personal data by social network users on their own walls would be something else entirely and could, in some cases, generate liabilities through the breach of the right to the protection of personal data. So, for example, the Spanish Data Protection Agency has recognised the preference of freedoms of expression and information in many

cases when they have come into conflict with the right to protect personal data.[34] It is no less true, however, that on some occasions the National High Court has reviewed this criterion, applying the judgment of proportionality[35] and estimating, in the specific case, the prevalence of the right to data protection, understanding that the information published would not, for example, require the accompaniment of a particular picture of a terrorist victim. However, when the person processing the personal data is a social network user on his or her own "wall", the Spanish Agency has proclaimed the guarantee of the right to protect personal data under the procedures of article 18 of the Data Protection Act, and ordered the manager of the social network to erase data.[36]

All the criteria detailed so far lead us to a judgment on the nature of the opinions, information and data placed on the wall of an online communications medium, in order to formulate the following considerations.

Firstly, whether the contents placed by the user on the mass media's online wall constitute a manifestation of the free expression of ideas or opinions or, whether they deal with true or genuine facts/information/data with certain public importance for the formation of public opinion must be taken into account. There are many questions we could explore on this point, but one can stand for all of them: does this apply equally to an individual who puts (personal or other) data on the wall of a communications medium via a social network as it does to the owners (professionals) of the communications medium in terms of the requirement for the constitutional conditions of the truthfulness and public importance of the "newsworthy event"? Today it is clear that the intensity of such a requirement is notably weakened (more often than not non-existent) in practice and that, probably, not to accept this would involve devaluing the extraordinary power generated in the forging of global public opinion by a large, anonymous mass of "information providers" who are consubstantial with the phenomenon of Internet users opening up the information society.

Secondly, and also not easy to resolve, the question is raised as to the delimitation of responsibilities for managing the content of the walls on a social network page managed by an online communications medium. Traditionally, the owner of a social network has been considered as a "provider of information society services" – as shown in the resolutions of the Spanish Data Protection Agency under the umbrella of the provisions established in the Spanish Information Society and Information

[34] For all of them, see Case Nº: E/00871/2005, http://bit.ly/nx7oMt

[35] "The image, then, is data covered by Act 15/1999, but a detailed examination of the case reveals that, although the quality of the images is not good, it can be understood that the processing of the image data has been excessive, considering that it is not covered by the consent of those affected (there is no evidence that they knew the images had been published); nor is it covered by freedom of information and, in any case, it seems that there has been a disproportionate use of the image as personal data, given that the newsworthy character of the information is sufficiently fulfilled without the need to include direct images of the sick. Instruction must therefore continue in relation to the possible unjustified use of image data." Decision dated 9 June 2009, of the First Chamber for Contentious Administrative Proceedings of the National High Court, handed down in appeal number 325/2008.

[36] See Proceedings Nº: TD/00690/2009. Available at http://bit.ly/n9DwdR

Society Services Act 34/2002, dated 11 July and in accordance with Opinion 5/2009 of the Art. 29 Working Party on Social Networks – which, in practice, would place it in a "neutral position" in the communication process without any responsibility being attributed to the technological tool or platform limited to hosting content provided by third parties. In other words, *a priori*, the owner of the social network (Facebook, Twitter, etc.) would be, for legal purposes, absolutely free of any liability that might be generated by the content (opinions, facts, personal data) provided by the users of the social network accounts and hosted on it. Now, in the circumstances that concern us, the social network account is open and managed by online mass media, but the content continues to be provided by individuals. Is it appropriate to also release the online mass media from liability for the content hosted for individuals or, on the contrary, does some kind of responsibility correspond to it (for example, *in vigilando*) if the content provided by the Internet user infringes applicable regulations and, in particular, the right to personal data protection?

For the questions set out as above, it is highly attractive to bring in the doctrine laid down by the Spanish Constitutional Court in its Decision 3/1997, when it judged the responsibilities that should be attributed to a newspaper on the content of the *Letters to the Editor* regularly included in such media. This involved circumstances which, *mutatis mutandis* would be paradigmatically integral to the problems we are analysing.

STC 3/1997 very precisely summarises the criterion of the Constitutional Court, concluding that the possibility of prior examination of the *Letters to the Editor* it publishes obliges it, firstly, to check the identity of the author of the "letter to the editor" as, if it does not, the editor of the communications medium assumes full responsibility for illicit content. Summarizing the judgment, *three key ideas* should be borne in mind: (1) the medium has a duty of diligence that takes the form of the duty to identify the author of content beyond the control of the medium to attribute to him/her full responsibility for the content he/she provides; (2) in the absence of this identification, spaces immune to possible breaches of fundamental rights would be created, and this would obviously be repugnant to the demands of the constitutional system for guaranteeing rights and freedoms; (3) the publication of content from outside without knowing the identity of the author implies that the medium accepts its content and any liabilities deriving from it.

But the above doctrine is as conclusive for traditional communications media practices as it is unviable in the digital environment we are analysing – as it risks blocking manifestations on the Internet (social networks) that maximise the requirements of freedom of information in modern democratic societies. The above doctrine would be impossible to apply to the context of a social network in that the very way it operates nowadays prevents any identification. In addition, the rapidity of publication of content and its volume make *a priori* control impossible – enforceable *a posteriori* liability for it would be a different matter.

Because of all this, as Opinion 5/2009 of the European Data Protection Authorities Working Party points out, in this case we are looking at the provision of an information society service subject, in Spain, to the Information Society and E-Commerce Services Act 34/2002, dated 11 July. As a result, when Spanish legislation applies,

the provider's liability will require the existence of two elements: (a) *Effective knowledge* of the illicit nature of the content from the time notice is received of a complaint through the complaints area on the social network, or when an authority, such as the AEPD, requires some kind of action. (b) *Absence of diligence* in the form of withdrawal of the illicit information.

Everyone is aware, however, that this is a complex situation going beyond legal analysis and transferring a certain ethical responsibility to the media: having multiplied the impact of freedoms of information by extending the possibility of exercising freedoms of expression and information to any member of the public and, taking account of the fact that the media themselves create, use and facilitate these new spaces on the social networks, it would be highly advisable for them to promote user training through ethical codes or usage rules.[37] This is particularly necessary in a context lacking specific regulations and with the difficulty of transferring traditional legal/constitutional categories to the digital environment, as shown by the common practice by citizens of exercising the right of erasure included in the personal data protection legislation. All this is to prevent the existence of "spaces immune" to Law that irresolvably prevent the effective guarantee of the right to protect personal data when the actions of mass media in a social network come into play.

References

Allen, Anita L. 2008. Dredging up the past: Lifelogging, memory, and surveillance. *The University of Chicago Law Review* 75.1: 47–74. http://lawreview.uchicago.edu/sites/lawreview.uchicago.edu/files/uploads/75.1/75_1_Allen.pdf. Accessed 19 Feb 2012.

Antonia, Paniza Fullana. 2009. Cuestiones jurídicas en torno a las redes sociales: Uso de datos personales para fines publicitarios y protección de datos de menores. *Revista Española de Protección de Datos* 6: 41–68.

Arnó Torrades, Ramón. 2011. La cancelación de los datos personales en las redes sociales: una aproximación práctica. In *Derecho y nuevas tecnologías. Primera parte. Nuevas tecnologías, sociedad y derechos fundamentales*, vol. 1, ed. Ana I. Herrán, Aitziber Emaldi Cirión, and Marta Enciso, 15–24. Bilbao: Universidad de Deusto.

Barriuso Ruiz, Carlos. 2009. Las redes sociales y la protección de datos hoy. *Anuario de la Facultad de Derecho de Alcalá de Henares* 2: 303–340.

Castells, Manuel. 2001. *La galaxia Internet. Reflexiones sobre Internet, empresa y sociedad*. Barcelona: Areté.

Cerezo, José M. 2006. *La blogosfera hispana: Pioneros de la cultura digital*. Madrid: Biblioteca de la Fundación France Telecom España.

Council of the European Union. 2011. Council conclusions on the protection of children in the digital world. doc. 2011/C 372/04. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2011:372:0015:0018:EN:PDF. Accessed 19 Feb 2012.

[37] See Spanish Data Protection Agency. INTECO. *Estudio sobre la privacidad de los datos personales y la seguridad de la información en las redes sociales online*. Madrid, 2009, page 92 (english version available in http://www.inteco.es/file/vuiNP2GNuMjfCgs9ZBYoAQ).

Díez López, Iban. 2011. Redes sociales y la Web 2.0: Privacidad y protección de datos. In *Derecho y nuevas tecnologías. Primera parte. Nuevas tecnologías, sociedad y derechos fundamentales*, vol. 1, ed. Ana I. Herrán, Aitziber Emaldi Cirión, and Marta Enciso, 463–474. Bilbao: Universidad de Deusto.

Dumortier, Franck. 2009. Facebook y los riesgos de la "descontextualización" de la información. *IDP: Revista de Internet, Derecho y Política* 9. http://idp.uoc.edu/ojs/index.php/idp/article/view/n9_dumortier/n9_dumortier_esp. Accessed 19 Feb 2012.

Esther, Mitjans Perelló. 2009. Derecho y nuevas tecnologías. Impacto de las redes sociales en el derecho a protección de datos personales. *Anuario de la Facultad de Derecho de Alcalá de Henares* 2: 111–132.

European Commission. 2011. Implementation of the safer social networking principles for the EU. http://ec.europa.eu/information_society/activities/social_networking/eu_action/implementation_princip_2011/index_en.htm. Accessed 19 Feb 2012.

Fumero, Antonio, Roca Genís, and Encinar Jesús. (Fundación Orange España, 2007) *Web 2.0*. http://www.fundacionorange.es/fundacionorange/analisisprospectiva.html. Accessed 19 Feb 2012.

García Sanz, Rosa María. 2011. Redes sociales online: Fuentes de acceso público o ficheros de datos personales privados (Aplicación de las Directivas de protección de datos y privacidad en las comunicaciones electrónicas). *Revista de Derecho Político* 82: 101–154.

Lessig, Lawrence. 2001. *El código y otras leyes del ciberespacio*. Madrid: Taurus.

Lessig, Lawrence. 2006. *Code version 2.0*. New York: Basic Books/Perseus Books Group.

López Jiménez, David. 2009. La protección de datos de carácter personal en el ámbito de las redes sociales electrónicas: El valor de la autorregulación. *Anuario de la Facultad de Derecho de Alcalá de Henares* 2: 239–276.

Marta, Morillas Fernández. 2010. La protección jurídica del menor ante las redes sociales. In *La protección jurídica de la intimidad*, ed. Angeles Jareño Leal and Francisco Javier Boix Reig, 361–380. Madrid: IUSTEL.

Martínez, Ricard. 2009a. El derecho fundamental a la protección de datos: Perspectivas. In *Internet, Derecho y Política. Las transformaciones del derecho y la Política en 15 artículos*, ed. Pere Fabra, 141–165. Barcelona: Editorial UOC.

Martínez, Ricard. 2009b. Los contenidos audiovisuales en la multidifusión digital. Nuevos retos para la protección de datos personales. In *Hacia un nuevo modelo televisivo. Contenidos para la televisión digital*, ed. Miquel Francés i Domenech, 83–95. Barcelona: Gedisa.

Martínez García, Laura, and Patricia Monteserín Leiva. 2011. El periodismo ciudadano como herramienta de democratización de los medios informativos digitales: Caso práctico de burgoshoy. In *La investigación en periodismo digital: Algunos trabajos desde el ámbito universitario*, ed. José Juan Verón Lassa and Fernando Sabés Turmo, 248–260. Zaragoza: Asociación de Periodistas de Aragón.

Martínez, Ricard. 2010. ¿Interrogantes jurídicos ante los Smartphone? *Actualidad Jurídica Aranzadi* 13: 822.

Mayer-Schonberger, Viktor. 2009. *Delete: The virtue of forgetting in the digital age*. Princeton: Princeton University Press.

Megías Terol, Javier. 2010. Privacy by design, construcción de redes sociales garantes de la privacidad. In *Derecho y redes sociales*, ed. Artemi Lombarte Rallo and Ricard Martínez, 319–334. Pamplona: Civitas.

Mendiguren Galdospin, Terese, Meso Koldo, and Jesús Pérez Dasilva. 2011. El papel de las redes sociales en el proceso hacia una nueva arquitectura de los medios de comunicación social. In *La investigación en periodismo digital: Algunos trabajos desde el ámbito universitario*, ed. José Juan Verón Lassa and Fernando SabésTurmo, 432–444. Zaragoza: Asociación de Periodistas de Aragón.

O'Hara, Kieron, Tuffield, Mischa, M., and Shadbolt Nigel. 2008. Lifelogging: Privacy and empowerment with memories for life. *Identity in the Information Society* 1. doi:10.1007/s12394-009-0008-4. Accessed 19 Feb 2012.

Palfrey, John, and Urs Gasser. 2008. *Born digital: Understanding the first generation of digital natives*. New York: Basic Books.

Rallo, Artemi. 2010a. Protecting privacy in a fast, evolving, more complex digital world. In *Trends in glogal communications: Riding the next digital wave*, 1–10. Barcelona: International Institute of Communications.

Rallo, Artemi. 2010b. Internet of the things: The importance of privacy oriented strategies. *The 2nd Internet Annual of Things Europe,* Brussels, 1–8.

Rallo, Artemi, and Ricard Martínez. 2010. *Derecho y redes sociales*. Pamplona: Civitas-Thomson Reuters.

Requejo Alemán, José Luis, and Herrera Damas, Susana. 2011. ¿Cómo crear comunidad a través de Twitter?: Nueve buenas prácticas en medios españoles *en La transformación del espacio mediático*. Actas del III Congreso Internacional de Ciberperiodismo y Web 2.0, 666–681. Bilbao: Universidad del País Vasco.

Rodríguez Damián, Amparo. 2009–2010. Problemática de las redes sociales. *Anuario de la Facultad de Derecho de Ourense* 1: 109–128.

Roig, Antonio. 2009. E-privacidad y redes sociales. *IDP: Revista de Internet, Derecho y Política* 9. http://idp.uoc.edu/ojs/index.php/idp/article/view/n9_dumortier/n9_dumortier_esp. Accessed 19 Feb 2012.

Romero Portillo, José. 2011. Redes sociales: un nuevo entorno de trabajo para los medios de comunicación tradicionales. In *La investigación en periodismo digital: Algunos trabajos desde el ámbito universitario*, ed. José Juan Verón Lassa and Fernando Sabés Turmo, 261–270. Zaragoza: Asociación de Periodistas de Aragón.

Sibilia, Paula. 2008. *La intimidad como espectáculo*. Buenos Aires: Fondo de Cultura Económica.

Trías Sagnier, Jorge. 1992. Informática y privacidad. ¿Se pueden poner puertas al campo? *Cuenta y razón* 63: 98–101.

Vela Sánchez-Crespo, Cayetana. 2008. La privacidad de los datos en las redes sociales. *Revista Española de Protección de Datos* 5: 231–272.

Vilasau Solana, Mónica. 2009. ¿Hasta dónde deben regularse las redes sociales? *Revista Española de Protección de Datos* 6: 105–138.

Xalabarder Plantada, Raquel. 2010. Redes sociales y propiedad intelectual. In *Derecho y redes sociales*, ed. Artemi Rallo Lombarte and Ricard Martínez, 335–354. Pamplona: Civitas.

Author Biography

Ann Cavoukian is recognized as one of the leading privacy experts in the world. An avowed believer in the role that technology can play in the protection of privacy, Dr. Cavoukian's leadership has seen her office develop a number of tools and procedures to ensure that privacy is strongly protected, not only in Canada, but around the world. She is involved in numerous international committees and advisory boards focused on privacy, security, technology and business, and endeavours to raise awareness on the importance of strengthening consumer confidence and trust in emerging technology applications. In 2011, Dr. Cavoukian was honoured with the prestigious *Kristian Beckman Award* for her pioneering work on *Privacy by Design* and privacy protection in modern international environments. www.ipc.on.ca

Delphine Christin graduated from the Ecole Nationale Supérieure de l'Electronique et ses Applications (ENSEA) and the Technische Universität Darmstadt in 2009. She is a PhD student at the Center for Advanced Security Research Darmstadt (CASED) since April 2009 and at Secure Mobile Networking Lab, TU Darmstadt since October 2009. Her research interests are privacy schemes, interfaces and metrics for mobile sensing applications.

Colette Cuijpers is assistant professor at TILT, the Tilburg Institute for Law, Technology, and Society (Tilburg University, the Netherlands). Her research concerns private law aspects of ICT applications such as the internet, smart metering and Location Based Services. Her primary interests are privacy and the protection of weaker parties, such as consumers, employees, patients and children. Colette has been involved in several large-scale EU projects such as Breaking Barriers to eGovernment, FIDIS and VIRTUOSO. She has published in several peer reviewed journals and is currently involved in a Dutch Commit project on Trusted Healthcare Services. Besides research, Colette is responsible for TILT's international Master Program Law & Technology.

S. Gutwirth et al. (eds.), *European Data Protection: Coming of Age*,
DOI 10.1007/978-94-007-5170-5, © Springer Science+Business Media Dordrecht 2013

Maria Luisa Damiani holds a Ph.D. in computer science from EPFL, Lausanne(CH) and a MS in Computer Science from University of Pisa (I). Her research focuses on location privacy enhancing techniques, location-based access control, and spatio-temporal data modeling. She is principal investigator for the University of Milan in the EU project MODAP (Mobility, data mining and privacy, http://www.modap.org) and national co-representative in the EU Cost Action IC0903 MOVE She has been co-organizer of the ACM SIGSPATIAL Workshop on Security and Privacy in GIS and LBS (2008–2011). Prior to joining the University of Milan as assistant professor, she worked for several years in major public and private organizations in Italy as researcher and project manager in EU-funded research projects.

Norberto Nuno Gomes de Andrade is a legal researcher, with a Ph.D. on the right to identity in the context of new and prospective technologies issued by the Law Department of the European University Institute (EUI, Italy). Norberto graduated in Law at the Faculty of Law of the University of Lisbon, and holds a Master's degree in International Relations and European Studies from the Central European University (CEU, Hungary), and a Master's degree in Research from the European University Institute. In 2007 he was a Visiting Scholar at the Singapore Internet Research Centre (SiRC) of Nanyang Technological University. He has also been involved in several research projects dealing with the interaction between human rights and new technologies, namely in Brazil and Italy. Previously he worked as a legal expert in the field of telecommunications at the External Relations Department of the Portuguese Regulatory Authority for Communications (ANACOM, Portugal). His research interests are focussed on law and technology (including digital environments and ambient intelligence, but also biotechnology, neuroscience, artificial intelligence and genetics), data protection and privacy law, intellectual property, philosophy of law and legal theory. In 2009, he co-edited and published "Law and Technology: Looking into the Future" – Selected Essays.

He joined the EC JRC-IPTS (Seville) in September 2010 and is focussing his work on the various legal aspects of digital identity.

Paul De Hert is professor of law at the Faculty of Law and Criminology of Vrije Universiteit Brussel. He is the Director of the research group on Fundamental Rights and Constitutionalism (FRC) and senior member of the research group on Law, Science, Technology & Society (LSTS). Paul De Hert is also associated-professor Law and Technology at the Tilburg Institute for Law and Technology (TILT)

Ralf De Wolf holds a Master in Sociology, obtained at the University of Ghent. He is a doctoral researcher at IBBT-SMIT/Department of Media and Communication studies at the Vrije Universiteit Brussel (Brussels, Belgium). His Ph.D., in Social Science, focuses on the relationship between identity, privacy and community in online and offline environments. He is especially interested in theoretical field of Symbolic Interactionism and the social construction of technology. As a user researcher he is involved in the SPION project (Security and Privacy for Online Social Networks), a 4-year project (1/1/2011–31/12/2014) in the SBO program for strategic basic research with societal goal, funded by IWT (government agency for Innovation by Science and Technology) in Flanders (Belgium).

Unai Diaz-Orueta holds a Psychology Ph.D. at the University of Deusto (Spain, 2006). He has been a clinical psychologist at Crownsville Hospital Center, Maryland (USA, 2000–2001), at Bermeo Psychiatric Hospital (Spain, 2001–2002) and at La Loma Geriatric Residence (Spain, 2003–2005). His doctoral dissertation 'Effects of psychological intervention in cognitive decline of residentialized elderly people' was published by UMI Dissertation Publishing, Ann Harbor, MI (USA). Since 2008, he works as a research psychologist in Fundacion INGEMA, in several projects related to ageing and physical disability, being mainly involved in users' evaluation and handling of ethical issues, including privacy and data protection. His areas of interest are the study of variables enhancing cognitive reserve, and the development of cognitive training and rehabilitation programs.

Rachel L. Finn is an Associate Partner at Trilateral. She has expertise in security, privacy, data protection, technology assessment and stakeholder engagement. Rachel is currently co-authoring a book for Routledge Press on the social impacts of surveillance technologies. She has a Ph.D. in sociology from the University of Manchester.

Michael Friedewald is senior researcher and head of the ICT research group at Fraunhofer ISI. He has a background in Electrical Engineering, Economics and Science and Technology Studies. He has been responsible for numerous studies on privacy and trust related to emerging sciences and technologies. He is currently co-ordinating three FP7 projects dealing with privacy aspects in the field of ICTs and security technologies (FP7 projects PRESCIENT, SAPIENT, PRISMS).

Christian Fuchs is chair professor in media and communication studies at Uppsala University. He is chair of the European Sociological Association's Research Network on Sociology of Communications and Media Research, co-founder of the ICTs and Society Network and editor of tripleC – Journal for a Global Sustainable Information Society. He is coordinator of Uppsala University's involvement in 2 EU FP7 projects and directing a project funded by the Austrian Science Fund FWF. His research fields are social theory and digital media & society. He is author of the books "Internet and society", "Foundations of critical media and information studies", "Social media. A critical introduction" (in preparation) and co-editor of "Internet and surveillance".

Andrea Gerino is a Research Assistant at the Computer Science Department of the University of Milan. Member of the EveryWare Laboratory of the same university, he is also co-founder of EveryWare Technologies, a startup focused on the development of privacy-aware mobile applications. His research interests cover the area of mobile data management with particular focus on privacy management in Location Based Services.

Daniel Lopez Gomez is post-doctoral researcher at LSTS Centre (Vrije Universitet Brussel). He graduated in Psychology (Universitat Autonoma de Barcelona) in 2000 and obtained a Ph.D. in Social Psychology (UAB) in 2009 with a thesis titled "Securing care: Networks, Immediacy and Independence in a Home Telecare Service". He has been trained as an STS ethnographer. He is lecturer at Universitat Oberta de Catalunya from 2009.

Daniel Guagnin joint the research group "security – risk – privacy" of the Centre for Technology and Society (Technical University Berlin) in 2010. He worked on EU projects PATS and SIAM. He received his magister in Sociology from the Albert-Ludwigs-University in Freiburg (Germany). His research focuses on privacy and free software.

Serge Gutwirth is a professor of human rights, legal theory, comparative law and legal research at the Faculty of Law and Criminology of the Vrije Universiteit Brussel. (VUB), where he studied law, criminology and also obtained a postgraduate degree in technology and science studies. Gutwirth founded and still chairs the VUB-research group *Law Science Technology & Society* (http://www.vub.ac.be/LSTS). He publishes widely in Dutch French and English. Amongst his recent co-edited publications are *Safeguards in a world of ambient intelligence* (Springer, 2008), *Profiling the European citizen* (Springer 2008), *Reinventing data protection?* (Springer 2009), *Data protection in a profiled world* (Springer, 2010) and *Computers, privacy and data protection: an element of choice* (Springer, 2011) and *European Data Protection: in good health ?* (2012). Currently, Serge Gutwirth is particularly interested both in technical legal issues raised by technology (particularly in the field of data protection and privacy) and in more generic issues related to the articulation of law, sciences, technologies and societies.

Leon Hempel is a senior researcher at the Centre for Technology and Society (CTS) at the Technical University of Berlin since 1999. His research areas are sociology of technology and innovation, security studies and evaluation methodology. He studied Political Science and Comparative Literature. In the last 10 years he continuously built up the social science security research at the CTS, establishing it as an independent research area. For an interim time he was also Managing Director of the Centre for Technology and Society. Since 2011, Hempel is member of the scientific management office of the CTS and scientific coordinator for security and innovation research.

Rob Heyman is a Ph.D. Student at SMIT (Studies on Media, Information and Telecommunication) – part of IBBT (Interdisciplinary institute for BroadBand Technology). He holds a master's degree in communication sciences and the philosophy of science. After graduating with a master thesis on online privacy and students, he started a Ph.D. on social media and privacy. This Ph.D. project is part of EMSOC (User Empowerment in a Social Media Culture), a 4 year Flemish research project (Belgium), investigating the empowering and disempowering role of social media on the levels of inclusion, literacy and privacy. His research is focused on the commodification of personal identifiable information via social media and the reaction of users to this process.

Matthias Hollick is heading the Secure Mobile Networking Lab (SEE-MOO) at the Computer Science Department of Technische Universität Darmstadt, Germany. He received his Ph.D. degree in 2004 from the TU Darmstadt. He has been researching and teaching at TU Darmstadt, Universidad Carlos III de Madrid (UC3M), and the University of Illinois at Urbana-Champaign (UIUC). In 2005, for his research,

he has received the Adolf-Messer Foundation award. His research focus is on secure and quality-of- service-aware communication for mobile and wireless ad hoc, mesh, and sensor networks.

Joshua B. Hurwitz is a Senior Research Psychologist at Motorola Mobility in Libertyville, Illinois, USA. He received a BA in Psychology from the University of Rochester and a MA and Ph.D. in Psychology from Harvard University. He specializes in cognitive, individual-differences, mathematical, and human-factors psychology, and has performed research in the areas of human learning and memory, risk taking, in-vehicle driver safety systems, and content personalization. His current research focuses on mitigating end-user privacy concern through more effective disclosure of privacy policies, enhanced user control over privacy, and adaptive privacy management. He has over 20 peer-reviewed publications and over 20 technical reports, as well as four patents.

Carla Ilten joined the Centre for Technology and Society as a junior researcher in 2008. She holds a Diplom in Sociology and Technology Studies from the Technical University Berlin. Carla Ilten is currently the junior project manager of the EU funded "Privacy Awareness through Security Organisation Branding" project. Her team coordinates the six partners in the project. Next to the privacy project, Carla Ilten's research focuses on technology activism. She has published a book on a Wireless Community Network as a case study of socio-technical innovation by civil society actors. In spring 2011, Carla Ilten worked with Prof. Hector Postigo at Temple University on an NSF funded project on the use of Web 2.0 media by activists for social change.

András Jóri, Ph.D. (40), attorney-at-law, data protection consultant, served as Parliamentary Commissioner for Data Protection and Freedom of Information of Hungary from 2008 to 2011. Previously, Dr. Jóri worked as an attorney, advising his clients on data privacy and IT law; he also did extensive regulatory work, advising the state and industry groups on many fields of IT and data protection law, as well as e-commerce, e-signatures, e-archiving, and e-procurement. He wrote the first commentary on data protection law in Hungary. Dr. Jóri has published widely about data privacy in Hungary and abroad, and is a frequent speaker at international conferences about data protection and freedom of information. He is also a certified system administrator.

Bert-Jaap Koops is Professor of Regulation & Technology at the Tilburg Institute for Law, Technology, and Society (TILT), the Netherlands. From 2005 to 2010, he was a member of De Jonge Akademie, a young-researcher branch of the Royal Netherlands Academy of Arts and Sciences. His main research field is law & technology, in particular criminal-law issues such as cybercrime, cyber-investigation powers, and DNA forensics. He is also interested in other topics such as privacy, data protection, identity, digital constitutional rights, 'code as law', human enhancement, and regulation of bio- and nanotechnologies. He co-edited six books in English on ICT regulation and published many articles and books in English and Dutch on a wide variety of topics.

Ronald Leenes is professor in Regulation by Technology at TILT, the Tilburg Institute for Law, Technology, and Society (Tilburg University). His primary research interests are privacy and identity management, regulation of, and by, technology. He is also involved in research in ID fraud, biometrics and Online Dispute Resolution. Ronald was work package leader in the EU FP6 PRIME project for socio-cultural aspects of privacy enhanced identity management. He is currently responsible for TILT's contribution to the FP7 project PrimeLife and leads the work package on social networks and collaborative workspaces. He has contributed to and edited various deliverables for the EU FP6 Network of Excellence 'Future of IDentity in the Information Society' (FIDIS).

Orla Lynskey is a Ph.D. candidate in law at the University of Cambridge, UK. Her doctoral research seeks to identify the objectives of European data protection law and queries whether a more harm-based approach should be taken to data protection regulation in the EU. In September 2012 Orla will take up a lectureship in law at the LSE, where she will teach Competition law, IT law and a course on Digital Rights, Privacy and Security. Prior to beginning her Ph.D. research, Orla worked as a teaching assistant at the College of Europe, Bruges (Belgium), a case handler in DG Competition at the European Commission and as an attorney in the antitrust department of a US law firm in Brussels.

Eugenio Mantovani holds a degree in Law from the University of Trento, Italy, and a LL.M degree on International and European Law from the Free University of Brussels (Vrije Universiteit Brussel, VUB), Belgium. Eugenio works as researcher and Ph.D. candidate at research group on Law Science Technology and Society, LSTS, at the Vrije Universiteit Brussel (VUB) and currently seconded experienced researcher at the Centre for Science, Society and Citizenship (CSSC) in Rome.

Ricard Martínez is Assistant Professor of Constitutional Law at the University of Valencia and has a Ph.D. in Law with the thesis "The impact of information technologies in fundamental rights". His main research issues are on data protection, privacy on internet, social networks, cloud computing and children. He is chairman of the Spanish Professional's Privacy Association and he was head of the Research Department of the Data Protection Spanish Agency (2007–2011). Author and coordinator of several monographs and comments to the Regulation of the Spanish Data Protection Act, about law and social networks and law and cloud computing. He is lecturer and teacher in the main master and events on this subject at Spain.

Sergio Mascetti is an assistant professor at the Computer Science Department, University of Milan. His primary research interests are privacy-preserving location and context based services. The main focus of his research involves the formal and technical issues, but he is also interested in the analysis of the legal basis and implications of his research. He is currently leading the research group at the University of Milan in the Italian project "*ENFORCE: Computer science and legal methods for enforcing the personal rights of non-discrimination and privacy in ICT systems*"

Anna Monreale holds a Ph.D., MS and BS degree in Computer Science from University of Pisa (2011, 2007 and 2004). She is currently a post-doc researcher at Department of Computer Science University of Pisa, Italy and a member of the Knowledge Discovery and Data Mining Laboratory (KDD-Lab), a joint research group with the Information Science and Technology Institute of the National Research Council in Pisa. She has been a visiting student at Department of Computer Science of the Stevens Institute of Technology (Hoboken, New Jersey, USA) (2010). Her research is in anonymity of complex forms of data including sequences, trajectories of moving objects and complex networks, and in privacy-preserving outsourcing of analytical and mining tasks. She has also been reviewer for several international data mining conferences and journals.

Shara Monteleone is a legal researcher, with a Ph.D. in Law and Information Technologies from the Media Integration and Communication Centre (MICC) of the University of Florence in 2007. She graduated in Law at the Law Faculty of Florence (Italy), and after a Masters degree in Communications Law, she worked as a post-doc researcher at INRIA (Grenoble, France), involved in particular in projects on privacy issues in Ambient Intelligence. She obtained a LL.M in Comparative, European and International Law from the European University Institute of Florence (EUI), focusing on Ambient Intelligence and the right to privacy – the case of detection technologies. As a university lecturer, she carried out several studies and participated in research projects in Media Law (with a constitutional and comparative law perspective) at the Department of Public Law (University of Florence and Universitad Autonoma de Barcelona), focusing on privacy and data protection regulation. Her previous working experiences include collaboration with the ITTIG-CNR (Istituto di Teoria e Tecnica dell' Informatica Giuridica, Centro Nazionale di Ricerca italiano), the Chamber of Commerce and with the Trade Union of Journalists of Florence. She has published several articles and participated as speaker in various conferences and workshops. She joined the EC JRC-IPTS (Seville) in May 2011, to work on the legal and economic assessment of e-ID services. She will focus on legal gaps in the existing digital identity regulatory framework.

Frank Pallas graduated in computer science at the Technical University of Berlin in 2004 and received his Ph.D. from the same institution in 2009 for a work on the economics of organization-internal information security. After his Ph.D., he changed to the Karlsruhe Institute of Technology where he has been working on different projects with regard to legal issues of smart grids and e-mobility with a strong focus on data protection and metrology law and is regularly consulted by different governmental agencies on the respective issues. Since 2010 he additionally holds a guest professorship for data protection and information economics at the Technical University of Berlin.

Martin Pekárek M.Sc., is a Ph.D. candidate at TILT, the Tilburg Institute for Law, Technology, and Society (TILT) (Tilburg University, the Netherlands). His research investigates privacy-enhanced e-ticketing solutions using location-based services. He is also involved in the EU COST Action *Living in Surveillance Societies (LiSS)*,

with the objective to increase and deepen knowledge about living and working in the surveillance age. Previously, he contributed to the FP7 project *PrimeLife* with a research focus on the technical and societal privacy aspects of social networking sites, leading to several international publications. Before joining TILT, Martin was employed as a management consultant to the telecommunications industry for more than 10 years.

Jo Pierson is professor in Use and Innovation of New Media in the Department of Media and Communication Studies at the Vrije Universiteit Brussel (Brussels - Belgium). He is also Senior Researcher and staff member at the research centre SMIT (Studies on Media, Information and Telecommunication) since 1996. In this position he coordinates the User Empowerment unit in the Digital Society research department of IBBT (Interdisciplinary Institute for Broadband Technology). In the past he has worked as researcher-advisor for the Dutch knowledge institute TNO in Delft. He holds a Ph.D. in Social Science (Media and Communication Studies) (2003). He lectures on undergraduate and master courses, covering socio-economic issues relating to the information society, digital media marketing and research methods. His research focus is on usage, innovation and privacy in new media. On these issues he has participated in over 50 national and international research projects, with 17 projects as promotor and 14 projects as co-promotor. He has been an expert for several government initiatives regarding ICT design and usage on European, Belgian and Flemish level.

Jörg Polakiewicz is head of the Human Rights Policy and Development Department in the Council of Europe, overseeing intergovernmental work related to human rights and bioethics and for over 3 years activities related to data protection Convention 108. He joined the organisation in 1993, working on constitutional reform in Eastern and Central Europe, as well as in the Council's legal service and head of the Law Reform Department. He is also a professor at the Europa-Institut of the University of the Saarland in Saarbrücken. From 1986 to 1993, he was a research fellow at the Max Planck Institute for Comparative Public and International Law in Heidelberg. In addition to numerous articles, he is co-editor of Fundamental Rights in Europe (Oxford University Press 2001), author of Treaty-making in the Council of Europe (Council of Europe Publishing 1999) and The Obligations of States arising from the Judgments of the European Court of Human Rights (Springer 1993).

Yves Poullet has been Rector of the FUNDP since September, 1st, 2010. Director of CRIDS since its creation in 1979 until August 31, 2010, he conducted various researches in the field of new technologies with a special emphasis on privacy issues, of individual and public freedom in the Information Society and of Internet Governance. Moreover, he is full professor at the Faculty of Law at the University of Namur (FUNDP) and Liège (Ulg). He has been during 12 years (1992-2004) member of the Belgian Commission on Data Protection (Commission belge de protection de la vie privée). In addition, he was since its origin, member of Legal Advisory Board of European Commission and the president of the

Task Force "Electronic Democracy and Access to public records". He is a founder of the European Telecommunication Forum, ECLIP and FIRILITE. He also chaired the Belgian Computer Association ABDI (Association Belge de Droit de l'Informatique).

Artemi Rallo is Chair of Constitutional Law at the Jaume I University of Castellón in Spain. He was also Professor of Constitutional Law and Head of the Public Law Department at the University from 1993 to 1998. Before his return to the university, he was Director of the Data Protection Spanish Agency. He graduated in Law with Extraordinary Prize Honours (1988) and has a Doctorate in Law from the University of Valencia (1990). He has authored numerous monographs, books and scientific articles in specialized national and international magazines. He has participated in research lines and projects on transformations of the Public Administration, electoral guarantees, threats to freedom of speech, protection of fundamental rights in the process of European integration and decentralisation in the Member States of the European Union. He was Director of the Center for Legal Studies of the Spanish Ministry of Justice from 2004 to 2007.

Annarita Ricci holds a Ph.D. in Civil Law and has been awarded a post doctoral research fellowship at the University of Bologna. Since 2005 she has been teaching Private Law and ICT Law in Master's programmes and courses. She has published several articles and collaborated in various collective volumes on Private Law and ICT Law.

Arnold Roosendaal LLM M.Phil., studied Dutch Law and obtained an LLM in Law and Technology at Tilburg University, the Netherlands. After his LLM, he followed a Research Master Programme at Tilburg University and KU Leuven, for which he obtained his M.Phil. Currently, Arnold is a Ph.D. Candidate at TILT, the Tilburg Institute for Law, Technology, and Society (TILT) (Tilburg University, the Netherlands). He has an interest in law and technology and the implications of technological developments on society. In his research he specifically looks at implications for individuals, often by analyzing effects on privacy and autonomy of the individual. Arnold has participated in several international research projects, such as FIDIS and PrimeLife, and has written several international publications. Next to that, he regularly participates in conferences as a speaker or panelist.

Jasper P. Sluijs is Ph.D. candidate at Tilburg Law and Economics Center (TILEC) (Tilburg University, the Netherlands). He submitted his dissertation on network neutrality and European law in June 2012. Previously, Jasper worked as a visiting scholar at the University of Pennsylvania, and was a research fellow with America's leading media reform organization Free Press in Washington, DC. He also was a Fulbright fellow at Georgia Institute of Technology's Digital Media department. Jasper's work has been published in the Federal Communications Law Journal, Telecommunications Policy, the Human Rights Law Review, and the European Journal of Law and Technology.

Daniel Trottier is a postdoctoral fellow in the Department of Informatics and Media. He previously held a postdoctoral fellowship in the Department of Sociology at the University of Alberta, Canada, and obtained his Ph.D. in the Sociology at Queen's University, Canada. Daniel's research considers relations between institutions and individuals as they are shaped by the domestication of new media technologies. His doctoral research examined social media surveillances, with Facebook as a case study. Daniel has authored several scholarly articles on surveillance, privacy, and technology, as well as the forthcoming book "Social Media as Surveillance" published by Ashgate.

Elena Urdaneta holds a Ph.D. in Pharmacy at Navarra University (1995, Spain). She made a series of postdoctoral visits to centres abroad including the UCLA Faculty of Medicine (Los Angeles, California) and the Physiology Department of the University of California in Irvine (UCI). She is the principal researcher on numerous funded research projects on physiology and gerontology and is the author or co-author of over 20 scientific research articles in international periodicals. She is a member of the Spanish Society of Physiological Sciences, Spanish Society of Geriatrics and Gerontology, International Society for the Advance of Alzheimer's research and treatment and of the American Physiological Society. She has managed ethical issues and worked as Ethical Issues Advisor in various FP6 and FP7 European projects.

David Wright is co-founder and Managing Partner of Trilateral. He has expertise in policy issues surrounding new technologies, risk, privacy, data protection, ethical and security issues. David is also a free-lance researcher on the faculty of VUB and has authored numerous articles in peer-reviewed journals. His latest book is *Privacy Impact Assessment*.