Law, Governance and Technology Series 20

Serge Gutwirth
Ronald Leenes
Paul de Hert *Editors*

Reforming European Data Protection Law

Springer

Law, Governance and Technology Series

Issues in Privacy and Data Protection

Volume 20

The *Law, Governance and Technology Series* is intended to attract manuscripts arising from an interdisciplinary approach in law, artificial intelligence and information technologies. The idea is to bridge the gap between research in IT law and IT-applications for lawyers developing a unifying techno-legal perspective. The series will welcome proposals that have a fairly specific focus on problems or projects that will lead to innovative research charting the course for new interdisciplinary developments in law, legal theory, and law and society research as well as in computer technologies, artificial intelligence and cognitive sciences. In broad strokes, manuscripts for this series may be mainly located in the fields of the Internet law (data protection, intellectual property, Internet rights, etc.), Computational models of the legal contents and legal reasoning, Legal Information Retrieval, Electronic Data Discovery, Collaborative Tools (e.g. Online Dispute Resolution platforms), Metadata and XML Technologies (for Semantic Web Services), Technologies in Courtrooms and Judicial Offices (E-Court), Technologies for Governments and Administrations (E-Government), Legal Multimedia, and Legal Electronic Institutions (Multi-Agent Systems and Artificial Societies).

More information about this series at http://www.springer.com/series/13087

Serge Gutwirth • Ronald Leenes • Paul de Hert
Editors

Reforming European Data Protection Law

Springer

Editors
Serge Gutwirth
Paul de Hert
Law, Science, Technology & Society (LSTS)
Faculty of Law and Criminology
at the Vrije Universiteit Brussel
Brussels, Belgium

Ronald Leenes
Tilburg Institute for Law, Technology,
and Society (TILT)
Tilburg University
Tilburg, The Netherlands

ISSN 2352-1902 ISSN 2352-1910 (electronic)
ISBN 978-94-017-9384-1 ISBN 978-94-017-9385-8 (eBook)
DOI 10.1007/978-94-017-9385-8
Springer Dordrecht Heidelberg New York London

Library of Congress Control Number: 2014954796

Printed on acid-free paper

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

Preface

The year 2014 is destined to be an important year for European Data protection. After lengthy discussions in the various committees, involving almost 4,000 amendments to the Commission's 2014 proposal, the European Parliament on 12 March 2014 adopted the proposal prepared by the committee chaired by MEPs Jan-Philipp Albrecht and Dimitrios Droutsas in the first reading. The waiting at the time of writing this foreword (June 2014) is for the position of the Council of Ministers on the Regulation. Once this is available, the European Parliament has to negotiate with the Council and the Commission on the final text.

The seventh annual Computers, Privacy and Data Protection (CPDP) conference was held in Brussels on 22, 23 and 24 January 2014, and was sharply influenced by the European Commission's new proposals and the discussions that led up to the almost 4000 amendments that were tabled by stakeholders within and outside Europe (e.g. the USA). The conference took place during a sort of 'interbellum'. At the time when contributors to the conference were preparing their papers and panels, the text of the draft Regulation was in flux. In October 2013, the European Parliament's influential LIBE Committee (Civil Liberties, Justice, and Home Affairs) had decided on the proposal to be forwarded to the Parliament. The LIBE version introduced changes to the original Commission proposal, for instance regarding the controversial 'right to be forgotten' provision (art. 17). As a result the legal reality at the conference differed from the one on which some authors based their texts.[1] Uncertainty regarding the final text of the Regulation also existed at the time of the conference itself; the European Parliament adopted the LIBE version in its first reading after the conference. And even when this volume will appear in print, we still may not know what the final Regulation will look like. This book volume reflects this state of affairs. It provides a reflection on the proposed changes in the data protection landscape that may appear outdated at the time of reading. The value of the contributions however remains because many of them extend beyond the actual regulation and hence have more principled value.

[1] This is nothing new. Legal reality constantly changes due to changing legislation and case law.

The present book is one of the results of the seventh edition of the annual Brussels based International Conference on Computers, Privacy and Data Protection: *CPDP2014 Reforming Data Protection: The Global Perspective*. The conference welcomed almost 850 participants at 'our' venue – the magnificent *Les Halles* – while another 500 people were reached through free public events organized in the evenings, also in Brussels. The 3-day conference offered participants 60 panels, several workshops and special sessions, with 343 speakers from academia, the public and private sectors, and civil society.

Under a slightly adapted title – *Reforming European Data Protection Law* – this volume brings together 16 chapters offering conceptual analyses, highlighting issues, proposing solutions, and discussing practices regarding privacy and data protection. The first part of the book contains two chapters on one of the prominent recurring CPDP themes: profiling. The second part focuses on one of the important new directions in the Regulation: a focus on preventing privacy risks and harms through impact assessments. It contains discussions on the tools and methodologies for impact assessments, as well as case studies. The third part contains three chapters on the controversial Right to be Forgotten. It addresses the history of the proposed right, ten reasons why it should be forgotten and explores one of the important dimensions in forgetting: time. The fourth part contains two chapters on the purported trade-off between privacy and security. The final, fifth, part deals with ways to support privacy and data protection. It contains a chapter discussing the nature of the Data Protection reform and a chapter on people's knowledge and awareness of privacy protection strategies. It furthermore offers three chapters on privacy by design and how to implement this in practice.

The chapters in this volume stem from two tracks. Six chapters (Chaps. 8, 9, 11, 13, 15 and 16) originate from responses to the conference's call for papers and have thus already been presented during the conference. The remaining chapters (Chaps. 1, 2, 3, 4, 5, 6, 7, 10, 12 and 14) were submitted by some of the conferences' 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 for their commitment and efforts: Rocco Bellanova, Colin Bennett, Paul Bernal, Laurent Beslay, Jean-François Blanchette Caspar Bowden, Ian Brown, Roger Brownsword, Peter Burgess, Denis Butin, Lee Bygrave, Jan Camenisch, Johann Cas, Roger Clarke, Claudia Diaz, Niels van Dijk, Simone Fischer-Hübner, Michael Friedewald, Lothar Fritsch, Raphael Gellert, Marieke de Goede, Seda Gürses, Rob Heyman, Mireille Hildebrandt, Dennis Hirsch, Joris van Hoboken, Chris Hoofnagle, Gerrit Hornung, Patrick Humblet, Paulan Korenhof, Eleni Kosta, Christopher Kuner, Marc Langheinrich, Marc van Lieshout, Gary T. Marx, Irma van der Ploeg, Charles Raab, Kjetin Rommetveit, Arnold Roosendael, Ronny Saelens, Joseph Savirimuthu, Jean Marc Van Ghyseghem, Diane Whitehouse, Brian Wynne and Tal Zarsky.

May this book meet the reader's expectations and contribute to the quality of the continuing debate about the future of privacy and data protection.

Brussels, Belgium — Serge Gutwirth
Tilburg, The Netherlands — Ronald Leenes
Brussels, Belgium — Paul de Hert
30 June 2014

Contents

Part III To Forget or Not to Forget? Or Is the Question: How to Forget?

Part IV Does It Take Two to Tango: Privacy and Security?

Part V Designing and Supporting Privacy and Data Protection

Contributors

Meg Ambrose is an Assistant Professor in the Communication, Culture and Technology department at Georgetown University. Her research interests focus on the governance of emerging technology and cover a wide range of technology policy issues including comparative censorship and privacy law, engineering and information ethics, robotics law and policy, and the legal history of technology. She earned her J.D. at the University of Illinois and her Ph.D. in Technology, Media and Society from the University of Colorado, Engineering and Applied Science. Email: megLeta@gmail.com.

Giampaolo Armellin is in charge of the Research Unit at CRG – Centro Ricerche GPI, the research centre of the GPI company, co-located at the EIT ICT Labs in Trento. He received his M.Sc. in Computer Science at the University of Milan. He has experience in the design and development of systems for industrial automation, process control, CRM, contact centres and ERP for healthcare. Currently, he manages the research team at CRG, working on research projects in eHealth and eWelfare domains. He has been one of the industrial representatives in the ALLOW project on pervasive computing and collaborates with the Information Engineering and Computer Science department of the University of Trento and the Fondazione Bruno Kessler. He is a member of the Advisory Board of the Design Thinking Centre (Doctoral Training Centre) on ICT for Quality of Life in Trento. Email: giampaolo.armellin@cr-gpi.it.

Jef Ausloos is a Doctoral Researcher at the University of Leuven, Faculty of Law (iMinds – ICRI). He has worked both in academia and civil society organisations in Hong Kong and the USA and holds law degrees from the University of Namur (B.A.), University of Leuven (M.A.) and University of Hong Kong (LL.M). Jef Ausloos has written on a variety of topics in the area of privacy law and media law. Currently, his research focuses on issues that lie at the intersection of Privacy and Data Protection, Freedom of Expression and Intermediary Liability on the Internet. In his Ph.D., Jef Ausloos is looking more closely at the distribution of control over personal data between online corporate entities and data subjects. Email: Jef.ausloos@law.kuleuven.be.

Eleonora Bassi is a Research Fellow of the Department of Information Engineering and Computer Science of the University of Trento and a Fellow at the Nexa Center for Internet and Society of the Polytechnic University of Torino. She holds a Degree in Law and a Ph.D. in Philosophy of Law at the University of Torino. After her Ph.D., she focused her interest on Information Law, Fundamental Rights and Data Protection Issues, and later on Public Sector Information European legal framework and regional policies. Currently, her research follows two main directions. First, the focus is on the new European Data Protection framework that will have a strong impact on privacy rights in digital environments and the circulation of personal data within the information market. Second, her work is on policy-oriented research on Open Data and Big Data. Email: bassi@disi.unitn.it.

Francesca Bosco is Project Officer within the Emerging Crimes Unit in UNICRI, the United Nations Interregional Crime and Justice Research Institute. She earned a law degree in International Law and joined UNICRI in 2006 as a member of the Emerging Crimes Unit. In her role in this organization, Bosco is responsible for fundamental rights protection projects and for cybercrime prevention and cybersecurity projects. She is currently acting as Programme Manager of the project 'PROFILING: Protecting Citizens' Rights against Illicit Profiling' funded by the European Union's Fundamental Rights and Citizenship program. She is one of the founders of the Tech and Law Center and she is currently a Ph.D. candidate at the University of Milan. Email: bosco@unicri.it.

Fabio Casati is a Professor of Computer Science at the University of Trento. He received his Ph.D. from the Politecnico di Milano and then worked for over 7 years in Hewlett-Packard, USA, where he was technical lead for the research programme on business process intelligence. He has also contributed (as software and data architect) to the development of several HP commercial products and solutions in the area of web services and business process management. In Trento, he is leading or participating in five FP7 projects, is active in many industry-funded projects, both local and international, and has over 20 patents. His passions are now in social informatics, or, informatics at the service of the community. His latest efforts are on IT for better living, on collaborative programming, and on models for scientific disseminations that can help scientists work in a more efficient way. Email: casati@disi.unitn.it.

Ann Cavoukian is recognized as one of the leading privacy experts in the world. Noted for her seminal work on Privacy Enhancing Technologies (PETs) in 1995, her concept of *Privacy by Design* seeks to proactively embed privacy into the design specifications of information technology and accountable business practices, thereby achieving the strongest protection possible. Among a number of her roles and awards, Dr. Cavoukian serves as the Co-Chair of the OASIS Privacy by Design Documentation for Software Engineers Committee whose goal is to enable software organizations to embed privacy into the design and architecture of IT systems, without diminishing system functionality. In 2011, she was honoured with the prestigious *Kristian Beckman Award* for her pioneering work on *Privacy by Design* and privacy protection in modern international environments. Email: Michelle.Chibba@ipc.on.ca.

Niklas Creemers is researcher at the Centre for Technology and Society (CTS) at Technische Universität Berlin (TUB). After graduating from University Duisburg-Essen, he worked in several research projects in security and privacy research, including projects like 'SuSI-Team: Passengers' Perceptions of Security in Public Transport Systems', 'SIMKAS-3D: Simulation of Cascading Crisis in Urban Critical Infrastructure Systems as a 3-D Model', and 'Dynamic Arrangements of Urban Cultures of Security – DynASS', all funded by the German Federal Ministry of Education and Research (BMBF). Furthermore Creemers participated in the EU-funded project 'PATS: Privacy Awareness through Security Organisation Branding'. He is currently part of CTS's research team on the project 'PROFILING: Protecting Citizens' Rights against Illicit Profiling' funded by the European Union's Fundamental Rights and Citizenship program. Email: creemers@ztg.tu-berlin.de.

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). Email: paul.de.hert@vub.ac.be.

Carolin Eicher is a bachelor student of Communication Studies at the University of Hohenheim, Germany, in her 5th semester. During winter term 2013/2014 she was part of a student research project within the Humboldt Reloaded 3.0 program at the Department of Media Psychology at the University of Hohenheim and thereby contributed to the development of the Online Privacy Literacy Scale (OPLIS).

Valeria Ferraris, Ph.D., is Research Fellow and Adjunct Professor in Criminology at the University of Turin. She is also a member of the board of Amapola, an agency that carries out research and interventions on security and urban liveability, liberties and rights. In 2008 she earned her doctorate in Criminology at the Catholic university in Milan. She is the author of several research reports and essays on immigration and crime, trafficking in human beings, urban security and human rights. She is currently working in the project 'PROFILING: Protecting Citizens' Rights against Illicit Profiling' funded by the European Union's Fundamental Rights and Citizenship program. Email: valeria.ferraris@amapolaprogetti.org.

Mona Fischer is currently pursuing a master's degree in communication management from University of Hohenheim, Germany, specializing in media psychology. In addition to her formal academic program, she also works as a student assistant at the Department of Media Psychology. Before arriving at University of Hohenheim, Mona Fischer completed her undergraduate degree in communication science and psychology at the Ludwig-Maximilians-Universität Munich, Germany.

Clara Fritsch cooperated on several national and international research on industrial relations and working conditions after studying sociology and political science. Since 2007 she is employed at the Austrian Union for Private Sector Employees, Graphical Workers and Journalists, mostly dealing with employees' data protection, ICT as a management instrument and blurring boundaries of work and privacy. Email: clara.fritsch@gpa-djp.at.

Christian Ludwig Geminn is a research assistant at the Project Group Constitutionally Compatible Technology Design (provet) at Kassel University. Having studied German and English Law (at Johannes Gutenberg-Universität Mainz and De Montfort University Leicester), his research interests lie inter alia with technology law and the relationship between liberty and security. Email: c.geminn@uni-kassel.de.

Alessio Giori received his M.Sc. degree in Computer Science, with specialization in 'Data, Media and Knowledge Management' from the University of Trento in Italy. He also received a professional master degree in 'Technologies for e-Government' and a bachelor degree in Computer Science from the same university. He is currently working at Fondazione Graphitech since on two European research projects called eENVplus and LIFE+IMAGINE. eENVplus is a Pilot Type A project, funded by European Union under the Competitiveness and Innovation Framework Programme – Information and Communication Technologies Policy Support Programme (CIP-ICT-PSP). LIFE+IMAGINE is a project co-funded by European Union under the LIFE+ Programme Environmental Policy and Governance in the framework of the objective 'strategic approach'. Email: alessio.giori@graphitech.it.

Ronald R. Grau is a Visiting Research Fellow at the University of Sussex where he obtained his D.Phil. in Computer Science and Artificial Intelligence in 2009. His research focuses on knowledge systems and representation design, complex process modelling, diagrammatic representation and reasoning, and the computational support of scientific discovery. For many years, Ronald Grau has also worked in commercial contexts, involving various technologies and applications, including knowledge integration, e-learning, graphics virtualisation, SaaS, databases, enterprise software, and business intelligence. In his role as Senior Researcher at Kingston University London, he worked on the EU FP7 project SIAM (Security Impact Assessment Measures) as a co-investigator. The project aimed to establish measures for evaluating technological solutions and their impact on society, and to make these measures accessible through a computational assessment support system. Email: r.r.grau@kingston.ac.uk.

Daniel Guagnin, M.A., is researcher at the Centre for Technology and Society (CTS) at Technische Universität Berlin (TUB). He is currently working in the PROFILING Project funded by the Fundamental Rights and Citizenship Scheme of the European Union. Before PROFILING, Guagnin worked in EU projects in the field of Privacy, Data Protection Accountability and Security Technologies, namely PATS and SIAM. His doctoral project focuses on the role of source code for the exchange of knowledge between software experts and lays in Free/Open Source Communities and is funded by a scholarship of the Konrad Adenauer Stiftung. Guagnin received his M.A. in Sociology from Albert-Ludwigs-University in Freiburg (Germany). Email: guagnin@ztg.tu-berlin.de.

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. 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. Email: serge.gutwirth@vub.ac.be.

Harry Halpin is a World Wide Web Consortium (W3C) Team member and a Research Scientist at the Computer Scientist and AI Lab at MIT, and a visiting researcher at Centre Pompidou. His technical and philosophical work is aimed at evolving the Web towards becoming a secure platform for free communication in order to enable collective intelligence. He received a Ph.D. in Informatics at the University of Edinburgh and author of the book *Social Semantics*, with over 40 publications in areas ranging from search engines to the philosophy of cognitive science. He is also President of the Board of LEAP (LEAP Encryption Access Project). Email: hhalpin@w3.org.

Leon Hempel, Ph.D., studied Comparative Literature and Political Science. He 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, risk and innovation as well as technology assessment. Currently he is carrying out two ethnographic studies focusing on control room practices in large infrastructure as well as on surveillance practices in the course of football matches. In the last 10 years he continuously built up the social science security research at the CTS on the basis of national, European as well as international research projects including URBANEYE, PATS and SIAM. Email: hempel@ztg.tu-berlin.de.

Alisa Hennhöfer is a bachelor student of Communication Studies at the University of Hohenheim (Germany) in her 5th semester. During winter term 2013/2014, she was part of a student research project within the Humboldt Reloaded 3.0 program at the Department of Media Psychology at the University of Hohenheim and thereby contributed to the development of the Online Privacy Literacy Scale (OPLIS).

Attila Kiss is a doctoral student and young researcher at the University of Pécs, Faculty of Law, Research Center for Information and Communication Technology Law, Hungary. Since 2011 he has participated in the Ph.D. programme specialized in IT and IP Law, and his research centres on the legal protection of the individual's appearance and the regulation of surveillance cameras in public places from the personal data protection aspect. Email: kiss.attila@ajk.pte.hu.

Bert-Jaap Koops is Professor of Regulation and Technology at the Tilburg Institute for Law, Technology, and Society (TILT), the Netherlands. His main research fields are cybercrime, cyber-investigation, privacy, and data protection. He is also interested in topics such as DNA forensics, identity, digital constitutional rights, 'code as law', and regulatory implications of human enhancement, genetics, robotics, and neuroscience. With a personal postdoc (1999), VIDI (2003) and VICI (2014) grant, Koops is one of the few Dutch researchers who received all three stages of NWO's (Netherlands Organisation for Scientific Research) personal research-grant scheme. Email: e.j.koops@uvt.nl.

Paulan Korenhof is a Ph.D. student at the Tilburg Institute for Law, Technology, and Society (TILT, Tilburg University) and at Privacy & Identity Lab (PI. Lab, a collaboration between Radboud University, SIDN, Tilburg University and TNO). In these institutes, Paulan works together with legal scholars, computer scientists, philosophers and social scientists. Both the interdisciplinary character of these institutes and the interdisciplinary scientific roots of Paulan herself (she holds a masters degree in both Philosophy and Public Law) shape her Ph.D. research in which she explores the problems caused for individuals by the 'memory' of the World Wide Web. She approaches this topic from an applied philosophy of technology perspective with an eye on the mutual shaping of law, technology and society. Email: P.E.I.Korenhof@uvt.nl.

Hans Lammerant has studied philosophy (VUB, 1996) and law (VUB/UIA, 2004). He also has a candidate degree in industrial engineering (1992) and is currently finalizing a Master in Statistics (UGent). Previously he has worked in civil society organisations on peace and human rights issues. In his research, he focuses on the effect of new developments in data science and statistics on surveillance and privacy. More generally he is interested in how technological developments and globalization influence the development of new forms of exercising power and how this impacts law. Email: hans.lammerant@vub.ac.be.

Ronald Leenes is Full Professor in Regulation by Technology at a the Tilburg Institute for Law, Technology, and Society (TILT), the Netherlands. His primary research interests are privacy and identity management, techno-regulation, applied data protection regulation, big data, conceptual analysis of privacy and data protection, and robotics and human enhancement. Currently his work focuses on accountability and transparency in big data and the cloud. He was responsible for TILT's research in several EU projects, such as PRIME, PRIMELIFE, ENDORSE, Robolaw and A4Cloud, and has contributed extensively to NoE FIDIS. Email: R.E.Leenes@tilburguniversity.edu.

Matthias Leese is a researcher at the International Centre for Ethics in the Sciences and Humanities (IZEW), University of Tuebingen. His primary research interests lie in the fields of critical security studies, privacy/data protection, surveillance studies and STS. Email: matthias.leese@izew.uni-tuebingen.de.

Laura Léonard is Consultant in the Department of Security and Privacy of *Deloitte Bedrijfsrevisoren/Réviseurs d'Entreprises*, Belgium, and assistant in commercial law at the University of Namur (UNamur). Laura is actively involved in the development and implementation of the Trademark Clearinghouse in the field of domain name industry and in various privacy and data protection projects in view of assessing privacy risks and helps companies reach compliance with data protection rules. Email: lauleonard@deloitte.com.

Fabienne Lind is a bachelor student of Communication Studies at the University of Hohenheim (Germany) in her 5th semester. During winter term 2013/2014, she was part of a student research project within the Humboldt Reloaded 3.0 program at the Department of Media Psychology at the University of Hohenheim and thereby contributed to the development of the Online Privacy Literacy Scale (OPLIS).

Christiana Markou is a Lecturer at the European University Cyprus and a practicing lawyer at Markou-Christodoulou & Polycarpou LLC, a law office based in Cyprus. She graduated from the University of Sheffield with an LL.B (Hons) in 1998 and an LL.M in 2000. She also holds a Ph.D. from the University of Lancaster awarded in 2011. Her research interests are mainly EU law, consumer protection law and information technology law. She currently is writing a book with Ashgate Publishing on agent technology in e-commerce and EU consumer protection law. Email: c.markou@euc.ac.cy.

Philipp K. Masur is a research assistant at the Department of Media Psychology at the University of Hohenheim, Germany. He is currently pursuing a Ph.D. in the field of media psychology. He studied communication science, business and philosophy at the University of Mainz, German, and the Macquarie University of Sydney, Australia. In his research, Philipp K. Masur focuses on how people manage their privacy in social media as part of their everyday practices. In his dissertation, he addresses how users of social media perceive situational factors of privacy and how far this perception influences privacy regulations and self-disclosure in the social web.

Alexander Roßnagel holds the Chair for Public Law with an emphasis on the law of technology and ecology at the faculty of economics at Kassel University, where he is also a Director of the Interdisciplinary Research Center for Information System Design (ITeG), Managing Director of the Competence Centre for Climate Change Mitigation and Adaptation (CliMA) and Scientific Director of the Project Group Constitutionally Compatible Technology Design (provet). Furthermore, he is a Fellow at the German Informatics Society (GI). Alexander Roßnagel has published extensively on all aspects of technology law and environmental law, and has served as a consultant for the German Federal Government on several occasions. Email: a.rossnagel@uni-kassel.de.

Giovanni Sartor is part-time Professor in Legal Informatics at the University of Bologna and part-time Professor in Legal informatics and Legal Theory at the European University Institute of Florence. He obtained a Ph.D. at the European University Institute (Florence), worked at the Court of Justice of the European Union (Luxembourg), was a researcher at the Italian National Council of Research (ITTIG, Florence), held the chair in Jurisprudence at Queen's University of Belfast, and was Marie-Curie Professor at the European University of Florence. He has been President of the International Association for Artificial Intelligence and Law. He has published widely in legal philosophy, computational logic, legislation technique, and computer law. He is Co-director of the *Artificial Intelligence and Law* journal and Co-editor of the *Ratio Juris* journal. His research interests include legal theory, logic, argumentation theory, modal and deontic logics, logic programming, multiagent systems, computer and Internet law, data protection, e-commerce, law and technology, aviation law, and human rights. Email: sartor@cirfid.unibo.it.

Georgia Skouma has practised as lawyer specialised in Information Technology, Communications and Privacy Law since 2001. She is currently Director in the Department of Security and Privacy of *Deloitte Bedrijfsrevisoren/Réviseurs d'Entreprises*, Belgium. Her role as business legal adviser with Deloitte is to help corporate clients in developing and implementing risk-based solutions and procedures to meet their legal obligations in a number of areas, primarily in data protection, information security, privacy and e-government. Email: gskouma@deloitte.com.

Elijah Sparrow is a longtime anti-surveillance activist and co-founder of riseup.net, a provider of secure communication alternatives for social movements. He is the primary inventor and lead technical architect of the LEAP Encryption Access Project software. He is also the lead programmer for the free software project Crabgrass, a social collaborative space for activist groups with a focus on security. His research areas include digital surveillance and the communication repertoires of social movements. Email: elijah@leap.se.

Jovan Stevovic is a researcher at Centro Ricerche GPI, a research centre of the GPI Company where he is working on different research and industrial projects in the healthcare domain. He received his Ph.D. in Computer Science from the University of Trento in 2014 with the thesis on methodologies and technologies to enable privacy-aware data sharing in healthcare. As past experiences he participated in the development of electronic health record and data warehousing systems in the Province of Trento, solving problems related to medical record sharing such as data and service integration, privacy and security. His current research activity is focused on solving regulatory compliance and privacy issues related to the healthcare data management in software as a service environment. Email: jovan.stevovic@cr-gpi.it.

Ivan Szekely, social informatist, senior research fellow of the Open Society Archives at Central European University, Associate Professor at the Budapest University of Technology and Economics, and board member of the Eotvos Karoly Policy Institute. His research interests are focused on information autonomy, openness and secrecy, privacy, identity, memory and forgetting, and archivistics. Email: Szekelyi@ceu.hu.

Gergely László Szőke is a researcher at the University of Pécs, Faculty of Law, Research Center for Information and Communication Technology Law, Hungary. He also works as the internal data protection officer of the University of Pécs. His research areas are data protection and freedom of information, e-commerce law, online dispute resolution and copyright law. Besides his teaching activity he participates in national and European research projects (e.g. PAW project). From 2010 to 2011 he worked as a part-time data protection expert at the Office of Hungarian Parliamentary Commissioner for Data Protection and Freedom of Information. Email: szoke.gergely@ajk.pte.hu.

Doris Teutsch is a research assistant and Ph.D. candidate at the Department of Media Psychology at the University of Hohenheim, Germany. She completed her studies with a Master of Science degree in Empirical Communication Studies at the University of Hohenheim. Prior to this she graduated from Ludwig-Maximilians-University Munich, Germany, with a Bachelor degree in Communication Science, with Sociology as minor subject and a semester abroad at Babes-Bolyai-University Cluj-Napoca, Romania. Her research focus is on privacy and self-disclosure in the social web.

Sabine Trepte is Professor for Media Psychology at the University of Hohenheim in Stuttgart, Germany. Her research focuses on online disclosures and privacy from a psychological perspective. Sabine currently investigates online privacy with two large-scale projects funded by the German Federal Ministry of Education and Research. Specifically she conducts a longitudinal study investigating privacy, disclosures, social support, and authenticity over time. With a network of international scholars that she founded in 2008, Sabine conducted a trans-cultural study on privacy and online disclosures in Germany, the USA, the UK, the Netherlands and China. In 2011, Sabine Trepte published the book *Privacy Online*. She holds an M.A. in Psychology and received her Ph.D. in Media Psychology. Email: sabine.trepte@uni-hohenheim.de.

Govert Valkenburg is an academic researcher working in the interdisciplinary field of *Science and Technology Studies*. He has investigated and published on a variety of technological fields, including human genomics, sustainable energy and privacy and security technologies. Across these fields of interest, he has attended to issues in the democratization of technological society, the functioning of expertise in democracy, and the theme of citizenship in technological societies. He is currently based at Maastricht University. Alongside his academic career, he works as a professional singer in classical and early music. Email: g.valkenburg@maastrichtuniversity.nl.

Gabriela Zanfir obtained her Ph.D. title in 2014 from the Faculty of Law of the University of Craiova, with the thesis 'The rights of the data subject regarding personal data protection'. Her research focuses on a legalistic approach to privacy and data protection, characterizing the two concepts in a functional way by applying to them classical legal concepts and by adapting the latter where necessary. She is also interested in the relationship between cloud computing and data protection. In 2012 she was a visiting researcher at the Tilburg Institute for Law and Technology, for 3 months. She won the Junior Scholar Award at CPDP 2014. Currently, she is working for the European Data Protection Supervisor. (She submitted the paper in this volume as an independent researcher, therefore she is the sole responsible for the content). Email: gabriela.zanfir@edps.europa.eu.

Part I
Profiling: A Persistent Core Issue of Data Protection and Privacy

Chapter 1
Profiling Technologies and Fundamental Rights and Values: Regulatory Challenges and Perspectives from European Data Protection Authorities

Francesca Bosco, Niklas Creemers, Valeria Ferraris, Daniel Guagnin, and Bert-Jaap Koops

Abstract This paper aims to map the field of profiling, its implications for fundamental rights and values, and the measures which are or can be taken to address the challenges of profiling practices. It presents a working definition of profiling and elaborates a typology of its basic methods. In the second section the paper gives an overview of the technological background of profiling to display how fundamental rights and values of European societies are endangered by the use of profiling. Finally the paper presents the findings of a questionnaire addressed to European DPAs on the current and future legal framework, the domains of application, the complaints and remedies procedures regarding the use of profiling techniques, the main risks and benefits for the fundamental rights, and citizens' awareness on this topic. These findings contribute important insights for the ongoing discussion on the regulation of profiling in Europe.

F. Bosco (✉)
Emerging Crimes Unit, UNICRI, Turin, Italy
e-mail: bosco@unicri.it

N. Creemers • D. Guagnin
Centre for Technology and Society (CTS), Technische Universität Berlin (TUB), Berlin, Germany
e-mail: creemers@ztg.tu-berlin.de; guagnin@ztg.tu-berlin.de

V. Ferraris
Law Department, University of Turin, Torino, Italy

Amapola Progetti per la sicurezza delle persone e delle comunità, Torino, Italy
e-mail: valeria.ferraris@amapolaprogetti.org

B.-J. Koops
Tilburg Institute for Law, Technology, and Society (TILT), Tilburg, The Netherlands
e-mail: e.j.koops@uvt.nl

S. Gutwirth et al. (eds.), *Reforming European Data Protection Law*,
Law, Governance and Technology Series 20, DOI 10.1007/978-94-017-9385-8_1

1.1 Introduction

The term "Big Data" is grounded in socio-technological developments, which began with the invention of the computer and has unfolded a rapidly growing dynamic over the past decades. Technological advancement has fueled the digitization of our societies by increasingly powerful infrastructures, basing on digital devices and software. Mediated communication today has mostly become digital communication, and information has consequently become easy to process and store as data, and is at the same time fluid and persistent. New potentials of gathering data raise hopes for developing more advanced ways to manage societies. The more we know the better we can control social processes and steer societal progress. At least that is what we are promised by "Big Data" proponents. "Big Data" appears to be a fetish, a crystal ball which allows those who use it to not just look into the future but to gain information which enables them to shape it at their needs.[1]

However, big data itself is not information but still mere data.[2] The more data we gather the harder it is to extract usable information as the huge amounts of data exceed human capabilities of consideration. Consequently data needs powerful tools to be utilized as a marketable resource. These tools are considered to be found in technologies such as data mining. They are supposed to turn "Big Data" into the new oil.[3]

Profiling can be understood as a specific data mining method. In this perspective profiling is regarded as an (semi-)automated process to examine large data sets in order to build classes or categories of characteristics. These can be used to generate profiles of individuals, groups, places, events or whatever is of interest. Profiles structure data to find patterns and probabilities. Using actuarial methods in this context is supposed to generate prognostic information to anticipate future trends and to forecast behavior, processes or developments. The aim is to develop strategies in order to manage uncertainties of the future in the present. In this regard, the

[1] See Fraunhofer. IAIS, *Big Data – Vorsprung durch Wissen. Innovations potenzial analyse*, http://www.bigdata.fraunhofer.de/content/dam/bigdata/de/documents/FraunhoferIAIS_Big-Data-Analyse_Doku.pdf, last accessed 01 April 2014. The programs of the world's largest ICT fair CeBIT 2014, the Big Data Days 2013, and the European Data Forum and the presentations given there, draw an interesting picture of the potentials the ICT industry attributes to "Big Data" and big data analytics: http://www.cebit.de/home, last accessed 03 April 2014, http://www.big-data-days.de, last accessed 03 April 2014, and http://2014.data-forum.eu/, last accessed 03 April 2014.

[2] Sasa Baskarada and Andy Koronios, "*Data, Information, Knowledge, Wisdom (DIKW): A Semiotic Theoretical and Empirical Exploration of the Hierarchy and its Quality Dimension*," in Australasian Journal of Information systems, Vol 18, No 1 (2013): 5–24.

[3] Karl-Heinz Streibich, "*Big Smart Data. Mehrwert für Unternehmen*" (paper presented at the Big Data Days, Berlin, Germany, November 11–12, 2013).

ideology of “Big Data” and analytical tools such as profiling can be understood as an important facilitator and part of a preventive paradigm which can be found in diverse societal contexts.[4]

Even though the reality of profiling might not live up to the expectations of its prophets,[5] the assumed potentials of gathering and processing data spawn the dream of overcoming human deficiencies with technology, these new technologies also draw fears and skepticism as they impose threats on some of the core values and principles of European societies. Key challenges which have been identified by scholars include infringements of democratic principles and the rule of law: Data gathering, exchange, and processing potentially harm central values like individual autonomy and informational self-determination as well as the fundamental rights of privacy, data protection, and non-discrimination.

This paper aims to map the field of profiling. It focuses on its implications for fundamental rights and values in different fields of application and on the assessment of the existing countermeasures to address the challenges of profiling practices. In the following section this paper proposes a working definition of profiling. The third section gives an overview of the technological evolution building the ground for the emergence of profiling, afterwards it is demonstrated how fundamental rights and values of European societies are endangered by the application of profiling in various contexts (Sect. 1.4). In Sect. 1.5 the legal regulation of profiling is sketched. Finally the paper presents the first findings of a questionnaire carried out by the project PROFILING,[6] in order to gain knowledge about European Data Protection Authorities’ awareness, attitudes, and activities regarding profiling and its societal impacts.

1.2 Profiling: Towards a Definition

Profiling is a highly evocative term with multiple meanings, used in both specialist and non-specialist contexts. Whereas the literature on statistics does not pay specific attention to definitions and tends to focus on technical aspects (e.g. data mining

[4] See Susanne Krasmann, “*Der Präventionsstaat im Einvernehmen. Wie Sichtbarkeitsregime stillschweigend Akzeptanz produzieren*,” in *Sichtbarkeitsregime: Überwachung, Sicherheit und Privatheit im 21. Jahrhundert*, ed. Leon Hempel, Susanne Krasmann and Ulrich Bröckling (Wiesbaden: VS Verlag, 2010), 53–70 and Pat O‘Malley, “*Risk, power and crime prevention,*” *Economy and Society* 21/3 (1992): 252–275.

[5] For some of the technical problems which harm the reliability of profiling results, see Daniel Guagnin, Leon Hempel and Justin Jung, “Evolution of Technologies in Profiling”, Working Paper, http://profiling-project.eu/wp-content/uploads/2013/08/Evolution-of-Technologies-in-Profiling_0208.pdf, last accessed 02 April 2014.

[6] The PROFILING project is funded from the European Union’s Fundamental Rights and Citizenship programme. The 2 year project started in November 2012. More information on the project can be found on the website http://profiling-project.eu.

techniques and predictive models), providing a definition appears an issue among socio-legal scholars and policy makers. However a widely shared definition has not yet emerged.

Gary T. Marx gave one of the oldest definitions of profiling in a paper that analyses systems of data searching. Profiling (defined by the author in contrast to "matching") is defined by stressing the logic behind it: "the logic of profiling is more indirect than that of matching. It follows an inductive logic in seeking clues that will increase the probability of discovering infractions relative to random searches. Profiling permits investigators to correlate a number of distinct data items in order to assess how close a person or event comes to a predetermined characterization or model of infraction".[7] According to the author's background, this definition is strictly related to the law enforcement domain.

Almost 10 years later, Roger Clarke defined profiling as a "dataveillance technique (. . .) whereby a set of characteristics of a particular class of person is inferred from past experience, and data-holdings are then searched for individuals with a close fit to that set of characteristics".[8]

A legal scholar, Bygrave again stressed: "profiling is the inference of a set of characteristics (profile) about an individual person or collective entity and the subsequent treatment of that person/entity or other persons/entities in the light of these characteristics".[9]

Later on, Mireille Hildebrandt was the one who put the best effort to precisely define profiling and its distinctive features and the working definition proposed here has built on her work. She defines profiling as "the process of 'discovering' patterns in data in databases that can be used to identify or represent a human or nonhuman subject (individual or group) and/or the application of profiles (sets of correlated data) to individuate and represent an individual subject or to identify a subject as a member of a group (which can be an existing community or a discovered category)."[10]

Profiling creates a new form of knowledge that makes visible patterns that are otherwise "invisible to the naked human eye".[11] They are based on correlations found in data sets, and cannot be "equated with causes or reasons without further

[7] Marx, Gary and Reichman Nancy. "*Routinizing the Discovery of Secrets: Computers as Informants*," in *American Behavioral Scientist*, 27, 4 (1984): 429.

[8] Clarke, Roger, "*Profiling: A Hidden Challenge to the Regulation of Data Surveillance*," in *Journal of Law and Information Science* 4, 2 (1993): p. 403.

[9] Bygrave, Lee A., *Data protection law: Approaching its rationale, logic and limits* (The Hague: Kluwer Law International, 2002), 301.

[10] Mireille Hildebrandt, "*Profiling and AML*," in *The Future of Identity in the Information Society. Challenges and Opportunities*, ed. Kai Rannenberg, Denis Royer and Andre Deuker (Heidelberg: Springer, 2009a), 275.

[11] Mireille Hildebrandt, "*Who is Profiling Who? Invisible Visibility*" in *Reinventing Data Protection?*, ed. Serge Gutwirth et al. (Dordrecht: Springer, 2009c), 241.

inquiry; they are probabilistic knowledge."[12] Profiling represents a shift from the idea that knowledge is the result of tested hypothesis. It generates hypotheses: "the correlations as such become the 'pertinent' information, triggering questions and suppositions".[13] Consequently profiling fosters new forms of generating and applying knowledge. Due to the growing capacities of databases, and capabilities of advanced analysis profiling procedures become increasingly complex. In this context the human role in interpreting data changes significantly.

As pointed out by Hildebrandt, profiling can be categorized into non-automated, automated and autonomic profiling. Non-automated profiling is a form of reasoning that does not rely on any process of automation. Automated profiling is based on "automated functions that collect and aggregate data" and develop into "automation technologies that can move beyond advice on decision-making, taking a load of low-level and even high-level decisions out of human hands."[14] Differently, autonomic profiling describes the process whereby the human role is minimized and the decision making process is entirely driven by the machine.[15] Autonomic profiling "goes one step further than automated profiling."[16] The machines drive the decision making process, providing for a readjusted environment based on their profiling and without calling for human intervention. Besides their degree of automation profiling methods can be distinguished by their object and application. Profiling can be applied as group profiling or individual profiling: the techniques that identify and represent groups can also focus on individuals.[17] Moreover profiling relies on data collected from one single person or group to apply the information derived from data processing to the same person or group – direct profiling – or it relies on categorization and generalisation from data collected among a large population to apply it to certain persons or groups – indirect profiling. Group profiling can also

[12] Gloria González Fuster, Serge Gutwirth and Ellyne Erika, "*Profiling in the European Union: A high-risk practice*," in *INEX Policy Brief* 10 (2010): 2.

[13] Gloria González Fuster, Serge Gutwirth and Ellyne Erika, "*Profiling in the European Union: A high-risk practice*," in *INEX Policy Brief* 10 (2010): 2.

[14] Mireille Hildebrandt, "*Defining profiling: a new type of knowledge?*," in *Profiling the European Citizens. Cross-Disciplinary Perspectives*, ed. Mireille Hildebrandt and Serge Gutwirth (Dordrecht: Springer, 2008), 28.

[15] See Mireille Hildebrandt, "*Profiling: from Data to Knowledge. The challenges of a crucial technology*," in *DuD Datenschutz und Datensicherheit* 30(9) (2006): 548–552 and Mireille Hildebrandt, "*Defining profiling: a new type of knowledge?*," in *Profiling the European Citizens. Cross-Disciplinary Perspectives*, ed. Mireille Hildebrandt and Serge Gutwirth (Dordrecht: Springer, 2008), 17–47.

[16] Mireille Hildebrandt, "*Profiling: from Data to Knowledge. The challenges of a crucial technology*," in *DuD Datenschutz und Datensicherheit* 30(9) (2006): 550.

[17] See Anton, Vedder, "*KDD: The challenge to individualism*," in *Ethics and Information Technology* (1999): 275–281 and Arnold Roosendaal, *Digital Personae and Profiles in Law. Protecting Individuals' Rights in Online Contexts*, Oisterwijk: Wolf Legal Publishers.

be classified as distributive group profiling or non-distributive group profiling.[18] A distributive group profile identifies a certain number of people having the same attributes. All the members of the group share the same characteristics. In contrast, a non-distributive group profile identifies a certain number of people who do not share all the attributes of the group's profile.

These distinctions give an idea of the different types of profiling and their application. The forms of profiling, which are subject of this article are automated and autonomic profiling and their various forms and fields of application.

The following proposed definition takes into account the preceding evolution of technologies in which profiling is embedded and focuses on the purpose profiling is being used for. It will be the basis for this paper:

> Profiling is a technique of (partly) automated processing of personal and/or non-personal data, aimed at producing knowledge by inferring correlations from data in the form of profiles that can subsequently be applied as a basis for decision-making.
>
> A profile is a set of correlated data that represents a (individual or collective) subject.
>
> Constructing profiles is the process of discovering unknown patterns between data in large data sets that can be used to create profiles.
>
> Applying profiles is the process of identifying and representing a specific individual or group as fitting a profile and of taking some form of decision based on this identification and representation.

1.3 Societal Consequences of Digitization

Advanced data analysis tools have established new social practices of knowledge production and have created new types of knowledge. We argue that the practices of profiling have facilitated and are part of a broader societal paradigm of prevention. We will elaborate on the societal implications of changing social practices through emerging profiling technologies as a ground for the examination of threats for fundamental rights and values of European societies in Sect. 1.4.

Observations made by human beings need to be written down to be made explicit. The written documentation of observations can be regarded as a first step to enable a generalized and objectified way of keeping information and exchanging it between individuals and institutions.[19] Digitized information, however, can be processed and analysed automatically so that information is easier and cheaper to store, process and analyse. An illustrative example of how exhaustive and expansive

[18] See Anton, Vedder, "*KDD: The challenge to individualism*," in *Ethics and Information Technology* (1999): 275–281.

[19] The important role the implementation of written files played as storage and medium for information but also as a symbol of power for the Inquisition trials in Italy is displayed by Thomas Scharff, "*Erfassen und Erschrecken. Funktionen des Prozeßschriftguts der kirchlichen Inquisition in Italien im 13. und frühen 14. Jahrhundert*. "in A*ls die Welt in die Akten kam. Prozeßschriftgut im europäischen Mittelalter*, ed. Susanne Lepsius and Thomas Wetzstein (Frankfurt a.M.: Vittorio Klostermann, 2008), 255–274.

the detailed documentation of people's activities and behaviour has been, is the comparison between digital data the NSA stores with the amounts of files the Stasi – German Democratic Republic's domestic secret service – produced. All the information captured throughout the Stasi history would fill about 48.000 cabinets covering approximately 0,019 km^2. The NSA's planned data centre in Utah will host about 5 zettabytes of data which could roughly be converted in about 42 quadrillion file cabinets covering 17 million km^2 – bigger than the European continent.[20] The example also shows the differing efforts needed to collect and archive data depending on whether using analog or digital data processing. While the Stasi needed to install microphones, hire staff to monitor and document people's behaviour to gain information about their habits, attitudes and social networks, in a digitized world a lot of that information can be monitored and stored on the fly through sensors, log data or user generated content. This shows that the digitization of communication and transactions does not only produce more data but also provides new kinds of information[21] which can be used to extract knowledge about individuals: their social relations, interests and activities. Once stored and made accessible via computer networks, data becomes easily exchangeable worldwide. At the same time it becomes hard to grasp how data is exchanged, which information is gained and by whom. Furthermore the specific mediums can store specific data. Certain elements which can be archived on paper cannot be archived digitally and vice versa. Moreover certain information can hardly be digitized respectively digitally analyzed, e.g. hand-written information, and smells. By that, archives have a filtering function which shapes the accessibility of information as data. But simplified storage and exchange of data are only one aspect of the ongoing process of digitization of everyday life. Beyond that advanced methods of data analysis have fundamentally changed the procedures of knowledge production through automation.

Another effect of the digitization of data becomes evident when we think of the different haptic and cognitive perceptions of digital versus analog files and folders. Different items and elements can be put in an analog or digital file, and at the same time, the availability of and the access to certain kinds of information fundamentally changes. In other words: accessing information at a (real) desktop is very different from accessing information when sitting in front of a computer screen. Paper folders can be touched and felt, digital files are browsed on a screen and can be searched by keywords. Consequently, the way of reasoning changes, as first findings of one of the case studies conducted in PROFILING show.[22] More interaction of the analyst is

[20] Open Data City, *Stasi versus NSA*, accessed February 27, 2014, http://apps.opendatacity.de/stasi-vs-nsa.

[21] Bert-JaapKoops, "*Technology and the Crime Society: Rethinking Legal Protection*," in *Law, Innovation & Technology*, 1, 1 (2009): 93–124.

[22] Technische Universität Berlin conducted a case study about the transformation of policing practices due to the application of data processing technologies. Expert interviews were conducted with scholars, civil rights activists, directors of security technology companies, a police representative, and a lawyer. Police as well as technology providers mentioned changes in the workflow and the

oriented towards computer interfaces and thus influenced by the way user interfaces are designed, information is presented, and how searches can be conducted.[23] The transformation of the human role in knowledge production processes is even more significant when it comes to examining large-scale databases. Learning algorithms are trained on specific data sets to build categories or to find patterns in the data. Assumptions or hypotheses made by the analyst play a minor role during data processing, they are to a certain degree hidden in the process of writing algorithms and training the algorithms. Finally, hypotheses are derived "from the material".[24] As a consequence implicit assumptions driving the actors during the selection of training data, preprocessing target data and suitable algorithms become invisible and the outcomes produced by "the data" seem objectified. Subjective assumptions and social norms are hidden in the technology during the process of automatization, while outcomes based on computed models and databases are often perceived as solid statistics and thus more objective than human interpretation.[25] This perception as objectified knowledge of computer-generated models supports the thesis of a general tendency of technology to make social norms more durable[26] and more specifically the thesis that social sorting becomes strengthened if mediated through technology.[27] Profiles, as mentioned above, can be seen as hypotheses. These hypotheses are inductive as they are not necessarily developed on the basis of a theory or a common sense expectation, but often emerge in the process of data mining. This can be regarded as a shift from a more traditional, rather assumption-

construction of theses from digitally stored information. The report of the case study's final results will be available at http://profiling-project.eu/.

[23] See Nina Degele, *Einführung in die Techniksoziologie* (Stuttgart, UTB, 2002), p. 167–168.

[24] The results software can draw from data material are dependent on the quality of the data sets, which are examined, including the selection and pre-processing of data. Major problems, especially regarding large-scale data sets which combine data from various sources, are poor data quality, data incompatibility, and biased data sets which corrupt data mining outcomes. Furthermore operators might not be familiar with such reliability problems. Consequently operators might not act properly upon these problems. See Ana Canhoto and James Blackhouse, "General Description of Behavioural Profiling," in *Profiling the European Citizens. Cross-Disciplinary Perspectives*, ed. Mireille Hildebrandt and Serge Gutwirth (Dordrecht: Springer, 2008), 47–63 and Bernhard Anrig, Will Brown, and Mark Gasson, "The Role of Algorithms in Profiling," in *Profiling the European Citizens, Cross-Disciplinary Perspectives*, ed. Mireille Hildebrandt and Serge Gutwirth (Dordrecht: Springer, 2008), 65–87.

[25] See Toon Calders and Indrė Žliobaitė, "*Why Unbiased Computational Processes Can Lead to Discriminative Decision Procedures*," in *Discrimination and Privacy in the Information Society*, ed. Bart Custers et al. (Berlin: Springer, 2013), 43–57.

[26] See Bruno Latour, "Technology is Society Made Durable," in *A Sociology of Monsters: Essays on Power, Technology and Domination*, ed. John Law (London: Routledge, 1991), 103–131.

[27] See Michaelis Lianos and Douglas Mary, "*Dangerization and the End of Deviance: The Institutional Environment*," in *British Journal of Criminology* 40, 2 (2000): 261–278 and Rosamunde van Brakel and Paul De Hert, "*Policing, surveillance and law in a pre-crime society: Understanding the consequences of technology based strategies*," in *Cahier Politiestudies* 2011–3 no. 20 (2011): 163–192.

driven approach to a discovery-driven approach to knowledge generation.[28] This shift results not only from growing data capabilities and advancing technological methods. Lyon argues that the conceptualization of social threats as actuarially identifiable and addressable risks and the desire for intelligence-led management of populations play a key role in the spread of profiling technologies.[29] In this context data mining is considered a key technology for risk assessment in various fields of application such as eHealth, airport security, and policing. Profiling techniques are used to identify categories and groups in order to assess risks and probabilities of certain future developments. The generated profiles can then be used to sort individuals, groups, events or processes in order to make them addressable for specific practices.[30] In this regard profiling is a technology to structure potential futures in order to make them governable in the presence. Therefore profiling is an important practice of a broader societal preventive paradigm, which is based on probabilistic knowledge used to manage social processes in the form of risk management.[31] By that profiling technologies provide means of control, which can be exercised for care and protection or coercion and repression.[32]

1.4 Profiling as a Threat for Fundamental Rights and Values

Even though the results of data mining are often limited reliable,[33] proponents claim that the potentials for managing social and technological processes in more efficient ways through data gathering and analysis are immense. They expect that the growing amount of data and increasingly advanced tools for examination will provide information which will allow organisations to identify, target, and act upon undesirable developments at an early stage – preferably before they occur.

[28] See Mireille Hildebrandt, "*Defining profiling: new type of knowledge?*," in *Profiling the European Citizens. Cross-Disciplinary Perspectives*, ed. Mireille Hildebrandt and Serge Gutwirth (Dordrecht: Springer, 2008), 17–47.

[29] See David Lyon, "*Surveillance as Social Sorting. Computer Codes and Mobile Bodies*," in *Surveillance As Social Sorting: Privacy, Risk, and Digital Discrimination*, ed. David Lyon (London: Psychology Press, 2003), 20.

[30] Profiling appears to create a dialectic form of practical knowledge, which is non-representative and representative, as defined in Sect. 1.2, at the same time. It is non-representative as profiles do not describe a given reality, but are detected by the aggregation, mining and cleansing of data. Nevertheless as these profiles are used to address populations according to this knowledge, they constitute them as a reality and thus do have a representative function.

[31] See Pat O'Malley, "*Risk, power and crime prevention*", *Economy and Society* 21/3 (1992): 252–275.

[32] Torin Monahan, "Surveillance as Governance: Social Inequality and the Pursuit of Democratic Surveillance," in *Surveillance and Democracy issue* (2010): 91–110.

[33] See Bernhard Anrig, Will Brown, and Mark Gasson, "The Role of Algorithms in Profiling," in *Profiling the European Citizens, Cross-Disciplinary Perspectives*, ed. Mireille Hildebrandt and Serge Gutwirth (Dordrecht: Springer, 2008), 65–87.

Preemptive policing, early detection of pandemic risks, and the prevention of tax fraud are examples of the societal benefits of the use of sophisticated data mining methods. Yet there is a downside to these opportunities implied by the technological evolution of digitization: it threatens key aspects of fundamental citizen rights, such as the rights to privacy, data protection and non-discrimination, and core values of European societies – democracy, the rule of law, autonomy and self-determination. As societies rely more and more on profiling methods to steer social and technological processes the urgency of dealing with these threats grows.

1.4.1 Fundamental Values

The clash between liberal democracy[34] and profiling is brought about by their inherent characteristics. Profiling is considered a glamour technology: it gives the idea that human beings can attain unforeseeable knowledge that allows making better decisions. But the dark side of profiling is that it makes "invisible all what cannot be translated into machine-readable data."[35] This means that the decision-making process is prone to be biased in the data collection phase and because of the complexity of the applied algorithms, human beings cannot properly intervene in repairing this bias. Consequently, "as far as the governance of people and things becomes dependent on these advanced profiling technologies, new risks will emerge in the shadow of the real time models and simulations these technologies make possible. What has been made invisible can grow like weeds."[36] In other words, not to consider some of the aspects of an issue can turn, at least, into ineffective and wrong decisions or, at most, in serious risks and damages for the population.[37]

Not only human intervention is reduced during the decision-making process, but also citizens do hardly have any access to the procedure behind the construction and application of profiles. This seriously hampers the quality of a liberal democracy because of the unbalanced distribution of power[38] and knowledge asymmetries[39] between the ordinary citizens, on the one hand, and the government on the other hand. Knowledge asymmetries are a common phenomenon but it reaches a new peak in profiling technologies. In most of the cases, citizens are not aware of the

[34] See Fareed Zakaria, "*The rise of illiberal democracy*," in *Foreign Affairs*, 76, 6 (1997): 22–43.

[35] Serge Gutwirth and Mireille Hildebrandt, "*Some Caveats on Profiling*," in *Data protection in a profiled world*, ed. Serge Gutwirth, Yves Poullet and Paul de Hert (Dordrecht: Springer, 2010.), 33.

[36] Ibid.

[37] As an example we can think of applying automated profiling to the health sector were the risks of taking wrong decisions could cost lives.

[38] See Daniel J. Solove, *Digital Person: Technology and Privacy in the Information Age* (New York: New York University Press, 2004).

[39] See Serge Gutwirth and Mireille Hildebrandt, "*Some Caveats on Profiling*," in *Data protection in a profiled world*, ed. Serge Gutwirth, Yves Poullet and Paul de Hert (Dordrecht: Springer, 2010.), 31–41.

information circulating and how they could be used in the future. In particular, when profiles are constructed from data that is not of the data subjects, information is used to take decisions about them without their involvement. So there is no easy protection on the horizon. Moreover some sophisticated profiling technologies like Behavioural Biometric Profiling (BBP) "do not require identification at all"[40] and by that increase this problem.

If the position that citizens enjoy versus the state is one of the indicators of the quality of a liberal democracy, the governmental use of profiling techniques seriously challenges some essential democratic features. This is not only related to the recognition of rights by the state, but also to the opportunities these rights entail for the full and free development and expression of citizens' personalities and their effective participation in democratic life. In this framework are placed the fundamental values of autonomy and self-determination. Against the backdrop of the discussion about profiling, self-determination acquires the specific meaning of informational self-determination, which means that an individual needs to have control over the data and information produced by and on him/her. This control is "a precondition for him/her to live an existence that may be said 'self-determined'."[41] As shown in the prior section digitization of everyday life has led to opaque ways of data gathering, exchange and processing. Consequently technologies like profiling do not leave much space for autonomy and self-determination.[42]

As in any other field, the application of profiling in healthcare can be helpful, yet harmful. eHealth and mHealth (electronic health and mobile health) technologies enable constant monitoring and profiling of persons' physical conditions, their activities, medical treatment, or diet. That way e- and mHealth-applications might help people to pick up healthier lifestyles as well as improve cures for illnesses and the individual treatment of diseases. At the same time there is potential for gathering information about patients' lifestyles from a hard to grasp range of sources that could be used for an actuarial assessment of lifestyles to build risk categories which are not only used for "individualized" treatments, but also to offer "individual" insurance fees or other incentives to make clients adapt certain lifestyles. Yet the categories on which these incentives are created by profiling are anything but individual. They derive from abstract calculations conducted under the premise of profit maximization and transfer this economic logic to individual lifestyle choices by rewarding behaviours assessed as low risk or healthy, while sanctioning the ones which are considered as increasing risks for accidents or diseases. Even though profiling in this context is supposed to empower healthy

[40] Mireille Hildebrandt, "*Who is Profiling Who? Invisible Visibility*," in *Reinventing Data Protection?*, ed. Serge Gutwirth et al. (Dordrecht: Springer, 2009c), 243.

[41] Antoinette Rouvroy and Yves Poullet, "*The right to informational self-determination and the value of self-development. Reassessing the importance of privacy for democracy*," in *Reinventing Data Protection?*, ed. Serge Gutwirth et al. (Dordrecht: Springer, 2009), 51.

[42] Mireille Hildebrandt, "*Who is Profiling Who? Invisible Visibility*," in *Reinventing Data Protection?*, ed. Serge Gutwirth et al. (Dordrecht: Springer, 2009c), 243.

lifestyles, it also undermines individuals' autonomy. It facilitates the economization of everyday life by addressing individuals as dividuals – bundles of risks and behavioural probabilities, reducing them to profiles.[43] eHealth is only one area in which this logic is executed. Risk factors or behavioural probabilities, which are identified and addressed, vary contextually as aims and scopes of profiling agents differ. "Although we are constantly being monitored in some way or another we do not live in an Orwellian 'Big Brother' dystopia. [. . .] Rather, an intricate network of small surveillance societies exists, often overlapping, connectable or connected, but each with their own features and rules."[44] What links these *small surveillance societies* is the idea to create knowledge gathered from certain populations which allows steering individuals, groups, and social processes. At this point autonomy and informational self-determination are closely interwoven as putting one at risk can jeopardize the other.

In policing, the development of preventive measures is a key argument for the implementation of growing capacities of gathering, exchanging and analyzing information. In Germany, police forces host large numbers of distinct databases for various purposes. They are fed and maintained by different institutions, such as the federal police organizations, state police organizations, or domestic secret services. The rules for gathering and exchanging data as well as for the access to the information for different institutions are hardly comprehensible. They are defined by federal data protection and criminal justice law (e.g., Bundesdatenschutzgesetz, Bundeskriminalamtgesetz, Strafprozessordnung), and various other laws and orders on state and federal level.[45] Beyond that several technical orders and so called "Errichtungsanordnungen" determine the architecture, use and purposes of data bases installed by the police.[46] This opaque framework still lacks a legal definition that covers data mining measures like profiling as stated by the German

[43] Gilles Deleuze, "Postskriptum über die Kontrollgesellschaften," in *Unterhandlungen 1972–1990*, Gilles Deleuze (Frankfurt a.M.: Suhrkamp, 1992), 254–262.

[44] Bert-Jaap Koops, "*Technology and the Crime Society: Rethinking Legal Protection*," in *Law, Innovation & Technology*, 1, 1 (2009): 104.

[45] See Deutscher Bundestag, *Automatisierte Strafverfolgung, Data Mining und sogenannte erweiterte Nutzung von Daten in polizeilichen Informationssysteme*n, Drucksache 17/11582, 22 November 2012, http://dip21.bundestag.de/dip21/btd/17/115/1711582.pdf, last accessed 26 March 2014.

[46] Even though "Errichtungsanordnungen" can be requested by citizens, an expert on political activism in TUB's case study reported that police refused to give him requested information as handing out this information would hamper police work. Additionally several answers of the German government to requests of members of the parliament regarding data gathering, storage and analytics conducted by German police forces show that essential information about this practice is kept secret in order to avoid infringement of police work. See Deutscher Bundestag, *Automatisierte Strafverfolgung, Data Mining und sogenannte erweiterte Nutzung von Daten in polizeilichen Informationssysteme*n, Drucksache 17/11582, 22 November 2012, http://dip21.bundestag.de/dip21/btd/17/115/1711582.pdf, last accessed 26 March 2014 and Deutscher Bundestag, *Computergestützte Polizeitechnik bei Polizeibehörden*, Drucksache 17/8544 (neu), 06 Feb 2012, http://dipbt.bundestag.de/dip21/btd/17/085/1708544.pdf, last accessed 01 April 2014.

Government.[47] This results in serious threats for informational self-determination and in particular cases it affects citizens' political participation and finally even the development of a liberal democracy. For example, the German federal police, Bundeskriminalamt (BKA), maintains databases for politically motivated offenders (distinguished as left, right and foreign offenders), which are fed by and accessible for the state police organizations (Landeskriminalamt, LKA). The information stored can be used for example to reconstruct social networks, allocate people to groups or institutions, or to identify people to be kept away from certain events of special interest, for instance NATO or G8 summits. First findings of interviews, conducted within a PROFILING case study,[48] with activists who are an involved in civil rights groups, show that interviewees considered data gathering, exchange and its use in the policing practice as non-transparent and by that intimidating, especially for people which are just starting to join civil rights groups. (Potential) activists do not know if and which information is gathered at which events, for which reasons, for whom this information is accessible, and how it might be used – or if it could lead to further police measures. This uncertainty may result in hindering the exertion of civil rights or lead to adaptive behaviour. Persons might change their behaviour in order to not seem conspicuous or suspicious and avoid to be linked with e.g. civil rights groups. Even though the technology used in this context cannot be considered as fully automated profiling, the computer-assisted data storage and representation already leads to opaque structures which undermine informational self-determination and restrain citizens' political participation. Furthermore it indicates challenges emerging from "predictive policing" approaches which aim on using (semi-)automatically generated profiles to score the risk of certain groups and individuals to commit particular crimes.

1.4.2 Fundamental Rights

The fundamental values presented before are strictly interrelated with the right to privacy and data protection and to the protection from discrimination. As clearly underlined by Rodotà, "the strong protection of personal data continues to be a 'necessary utopia' if one wishes to safeguard the democratic nature of our political

[47] See Andrej Hunko, *Suchbewegungen zu Data Mining-Software gehen über gesetzlichen Auftrag des BKA hinaus*, 17 March 2014, http://www.andrej-hunko.de/presse/1934-suchbewegungen-zu-data-mining-software-gehen-ueber-gesetzlichen-auftrag-des-bka-hinaus, last accessed 26 March 2014, and Deutscher Bundestag, *Automatisierte Strafverfolgung, Data Mining und sogenannte erweiterte Nutzung von Daten in polizeilichen Informationssystemen*n, Drucksache 17/11582, 22 November 2012, http://dip21.bundestag.de/dip21/btd/17/115/1711582.pdf, last accessed 26 March 2014.

[48] For information about the case study conducted by Technische Universität Berlin see footnote 22.

systems."[49] Data protection is necessary in a democratic society, as Rouvroy and Poullet pointed out, to sustain a vivid democracy. The right to non-discrimination is equally important.[50] It is not by chance that the European Court of Justice, in two recent profiling-related cases[51] has invoked both the legislation on Data Protection and anti-discrimination to protect citizens' rights.

1.4.2.1 The Right to Privacy and the Right to Data Protection

Leaving aside all difficulties of defining the various notions of privacy[52] it is useful to shortly revisit the interplay between privacy and data protection. Following Gellert and Gutwirth, most privacy definitions[53] can be summarized in either the problem of being left alone, or the question of how to cope with information stemming from social interaction in a way that certain areas of one's personal life are hidden from unwanted views.[54] Data protection law however is made to ease the free flow of information by safeguarding personal data. In this respect privacy is a matter of opacity while data protection is related to transparency.[55] In the field of profiling it is highly relevant to consider the scope of both terms: while privacy is broader in the sense that privacy covers more than mere personal data the misuse of personal data can affect much more than someone's privacy. As outlined above various technologies nowadays potentially create digital data which can be part of automated processing and profiling. Accordingly the concepts of privacy and data protection are

[49] Stefano Rodotà, "*Data Protection as a Fundamental Right*", in *Reinventing Data Protection?*, ed. Serge Gutwirth et al. (Dordrecht: Springer, 2009), 78.

[50] See Antoinette Rouvroy and Yves Poullet, "*The right to informational self-determination and the value of self-development. Reassessing the importance of privacy for democracy*", in *Reinventing Data Protection?*, ed. Serge Gutwirth et al. (Dordrecht: Springer, 2009), 57.

[51] Huber v. Germany, C-524/06 (2008), find a summary of the judgment at: http://ec.europa.eu/dgs/legal_service/arrets/06c524_en.pdf; Test-Achats v. Council of Ministry, C-236/09 (2011), find a summary of the judgment at: http://ec.europa.eu/dgs/legal_service/arrets/09c236_en.pdf

[52] See Daniel J. Solove, "*I've Got Nothing to Hide' and Other Misunderstandings of Privacy*", in *San Diego Law Review* Vol. 44 (2007): 754–764.

[53] There is a large amount of literature on privacy taxonomies. Finn, Wright, and Friedewald summarizes the debate and propose a taxonomy of 7 types of privacy: 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). See Rachel L Finn, David Wright and Michael Friedewald, "*Seven Types of Privacy*", in *European Data Protection: Coming of Age*, ed. Serge Gutwirth et al. (Dordrecht: Springer, 2013), 3–32.

[54] See Raphael Gellert and Serge Gutwirth, "*Beyond accountability, the return to privacy?*," in *Managing Privacy through Accountability*, ed. Daniel Guagnin et al. (Houndmills: Palgrave Macmillan, 2012), 261–284.

[55] See Raphael Gellert and Serge Gutwirth, "*Beyond accountability, the return to privacy?*," in *Managing Privacy through Accountability*, ed. Daniel Guagnin et al. (Houndmills: Palgrave Macmillan, 2012), 261–284.

increasingly challenged by the capabilities of data usage and analytics. The concepts evolve over time as technologies develop and have to catch up with the constant progress: "its content varies from the circumstances, the people concerned and the values of the society or the community."[56] Moreover profiling technologies, as shown in this paper, lead to more black boxing, more opacity of data processing. It is in fact questionable how the factual use of data can be made transparent.

In order to build an exhaustive framework of the threats towards the right to privacy and the right to data protection, the OECD Privacy Principles[57] are taken as term of reference as one of the most comprehensive and commonly used privacy frameworks.[58]

These principles include (1) Collection Limitation Principle: data should be obtained by lawful and fair means and with the knowledge or consent of the data subject; (2) Data Quality Principle: data which are to be used, should be accurate, complete and kept up-to-date; (3) Purpose Specification and (4) Limitation Principle: The purposes for data collected should be specified only be used for the specified purposes; (5) Security Safeguards Principle: Personal data should be protected by reasonable security safeguards; (6) Openness Principle: There should be a general policy of openness about developments, practices and policies with respect to personal data. (7) Individual Participation Principle: Individuals should have the right: (a) to obtain the data stored relating to them; (b) to be informed about data relating to them (c) to be given reasons if a request made under subparagraphs (a) and (b) is denied, and to be able to challenge such denial; and (d) to challenge data relating to them and, if the challenge is successful to have the data erased, rectified, completed or amended. (8) Accountability Principle: A data controller should be accountable for complying with measures, which give effect to the principles stated above.[59]

[56] Pierre Trudel, "*Privacy Protection on the Internet: Risk Management and Networked Normativity*," in *Reinventing Data Protection?*, ed. Serge Gutwirth et al. (Dordrecht: Springer, 2009), 322.

[57] The Privacy Principles are contained in the OECD Guidelines on the protection of privacy and transborder flows of personal data. In 2013 these Guidelines have been updated; the original version, developed in the late 1970s and adopted in 1980, was the first internationally agreed upon set of privacy principles. See OECD, *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, accessed 14 March, 2014, http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm.

[58] The basic data protection principles largely overlaps with the principles outlined in the Council of Europe's Convention 108 for the Protection of Individuals with Regard to Automatic Processing of Personal Data (http://www.conventions.coe.int/Treaty/en/Treaties/Html/108.htm) and the Directive 95/46/EC on the Protection of Personal Data (http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML), however the OECD Guidelines already included the principle of accountability which has been prominently resumed in the Article 29 Working Party's Opinion on the Principle of Accountability in 2010 (http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp173_en.pdf, all accessed 03 March 2014).

[59] Data protection accountability has recently been debated among privacy scholars (See Daniel Guagnin et al., eds, *Managing Privacy Through Accountability* (Houndmills: Palgrave, 2012.)) and is taken into account in the discussions of the current draft of the GDPR.

RFID-enabled travel cards (as used in many metropolis, e.g. Oyster Card in London and Octopus Card in Hong Kong) can serve as an example to display how new technologies challenge the right to privacy and data protection. The cards contain personal information about their holders so that they can be allocated to a single person to avoid abuse by others. Beyond that the RFID chips can be used to generate sophisticated traveler profiles,[60] or even consumer profiles, where the cards can also be used to pay in shops. Furthermore traveling profiles could be used to find suspicious traveling patterns, revealing potentially deviant behaviour (e.g. people which are using uncommon amounts and combinations of subway stations indicating activities from drug dealing to infidelities, as illustrated in Doctorow's Novel "Little Brother"). This shows that data which is not conceived as sensitive or potentially harmful can become such through combinations with other data.[61] Even data which is anonymized or de-identified can be used to generate outcomes which lead to issues from privacy infringements to discrimination. Furthermore the effectiveness of those approaches is doubted by scholars. Big Data analytics allow to draw unpredictable inference from information and by that undermine strategies of de-identification as by combination of anonymized data identities can be reconstructed.[62] New technologies such as RFID-chips make it difficult to keep track of which information is collected for which purposes and to keep track of the factual use of such data. The temptation for those gathering data to use it in new ways and generate new knowledge is high, and getting aware of such (unspecified) use can be very difficult. The discussions about putting data protection into practice through measures of accountability aims on making the use of data proactively transparent and traceable, but the practical implication is complicated.[63] There is

[60] Some RFID chips which use unique identifiers for initializing connections to RFID readers can also be tracked by third parties through this unique ID without any need to establish an authorized connection with the chip. See for instance http://www.spiegel.de/netzwelt/netzpolitik/sparkassen-pilotprojekt-kontaktlose-geldkarte-verraet-ihren-besitzer-a-831711.html.

[61] For a problematisation of inferring private data from large databases and efforts to avoid disclosure of private data see LiWu Chang and Ira S. Moskowitz, "An Integrated Framework for Database Privacy Protection", in *Data and Application Security*, ed. By Bhavani Thuraisingham et al., IFIP International Federation for Information Processing 73 (Springer US, 2001), 161–72; Stefan Sackmann, Jens Strüker, und Rafael Accorsi, "Personalization in Privacy-aware Highly Dynamic Systems", *Commun. ACM* 49, Nr. 9 (September 2006); Vassilios S. Verykios et al., "State-of-the-art in Privacy Preserving Data Mining", *SIGMOD Rec.* 33, Nr. 1 (März 2004): 50–57.

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

[63] Some scholars critizice that accountability could become just another ineffective bureaucratic measure, yet other scholars see potential of achieving stronger communication about data processing practices and verifiable accounts of data processors. The impact and effectiveness of accountability will depend on the actual implementation and the adoption by data processors. A number of contributions to the debate of the principle of accountability can be found in Daniel Guagnin et al., eds, *Managing Privacy Through Accountability* (Houndmills: Palgrave, 2012).

a general lack of transparency in profiling techniques[64] and also data processor's accountability is challenged by opaque practices and black boxed technologies inherent to data mining and profiling. This makes both the Security Safeguards Principle and the Openness Principle far from being taken into consideration. Individuals become more and more transparent, as public bodies, and even private companies, become more and more intrusive, moving on legal borderlines.

1.4.2.2 The Right to Non-discrimination

The right to non-discrimination "emanates from the general postulate of the equal dignity of human beings."[65] It constitutes a general principle in EU Law and lately has been enshrined as a fundamental right in Article 21 of the EU Charter of fundamental rights. It consists of a general principle of equality (i.e. similar situations have to be treated in the same way and different situations have to be treated differently) and of specific provisions developed in anti-discrimination legislations related to certain protected grounds (e.g. age, race, gender, religion, sexual orientation, etc.) and specific domain of application (i.e. labour market, vocational training, education, social security, health care, access to goods and services, criminal law).

The basic conceptual distinction in EU law is that between direct and indirect discrimination, both of which are prohibited in the EU law. Direct discrimination occurs when a person is treated less favourably than another and this difference is based directly on a forbidden ground. Indirect Discrimination occurs when apparently neutral criteria, practices or procedures have a discriminating effect on people from a particular protected group. This distinction is highly relevant in the context of profiling because rarely does the classification and categorization made by profiling techniques occur directly on forbidden grounds. More often the categorization is based on algorithms used to classify some attributes that can result as proxies of a protected ground. As stated by Romei and Ruggieri "the naive approach of deleting attributes that denote protected groups from the original dataset does not prevent a classifier to indirectly learn discriminatory decisions, since other attributes strongly correlated with them could be used as a proxy by the model extraction algorithm."[66] The best-known example is the one of "redlining", which

[64] See Mireille Hildebrandt, "*Profiling and AML*," in *The Future of Identity in the Information Society. Challenges and Opportunities*, ed. Kai Rannenberg, Denis Royer and Andre Deuker (Heidelberg: Springer, 2009a), 273–310 and Mireille Hildebrandt, "*Technology and the End of Law*," in *Facing the Limits of the Laws*, ed. Erik Claes, Wouter Devroe and Bert Keirsbilck (Heidelberg: Springer, 2009b), 443–465.

[65] Melik Özden, "*The Right to non-discrimination*," in *Series of the Human Rights Programme of the CETIM* (2011): 7.

[66] Andrea Romei and Salvatore Ruggieri, "*Discrimination Data Analysis: A Multi-disciplinary Bibliography*," in *Discrimination and Privacy in the Information Society. Data Mining and Profiling in Large Databases*, ed. Bart Custers et al. (Berlin: Springer, 2013) 121.

is explicitly forbidden by US law. Redlining is used to identify the practice of denying products and services in particular neighbourhoods, marked with a red line on a map. Due to racial segregation or increasing demographic concentration of people similar for social class, employment condition and even nationality, people living in a particular neighbourhood may belong to a specific racial group or an ethnic minority. Hence, an apparently neutral attribute such as ZIP Code may turn into an indirect discrimination situation. In general profiling applied to marketing (web marketing, loan market, price determination, etc.) can easily hide practices of indirect discrimination. For this reason the research on data mining techniques that prevent discrimination (a kind of "discrimination proof data mining") is a fruitful research field.[67]

Another example is the smart approach to border surveillance. It relies on the use of technologies to automatically check the passengers at the border (so called smart borders). This use of technology consists of databases, sophisticated tools such as body, iris scanners and comprehensive programme of surveillance (e.g. Eurosur) whose final aim is to speed up border crossing for bona fide travellers, fight against illegal migration and enhance security. The proposed databases (Passenger Name Record, Registered Traveller Programme, Entry/Exit System) rely on an extensive collection of personal and non-personal data in order to differentiate among welcome and unwelcome travellers. Besides the risks related to privacy and data protection due to the use of biometrics and the lack of respect of the principle of purpose-binding and use limitation, the opacity of the logic behind the data mining procedure is in itself hard to harmonize with the obligation not to discriminate on prohibited grounds and above all raise huge concerns on the respect of human dignity.

The manifold risks which profiling imposes on fundamental values and rights as well as the complex effects of the implementation of this technology show that it is a challenge to provide adequate measures to protect European values and rights. The next section gives a brief overview of the state of this process in Europe.

1.5 So Far so Good – Regulating Profiling

In the current EU data protection legislation the word profiling does not appear. However. Article 15 of the Directive 95/46/EC (hereinafter, Data Protection Directive, DPD) concerns 'automated individual decisions' and thus is closely related to profiling. According to article 15(1): "every person has the right not to be subject to a decision which produces legal effects concerning him or significantly

[67] See Dino Pedreschi, Salvatore Ruggieri, and Franco Turini, "*The Discovery of Discrimination*," in *Discrimination and Privacy in the Information Society. Data Mining and Profiling in Large Databases*, ed. by Bart Custers et al. (Berlin: Springer: 2013), 91–108.

affects him and which is based solely on automated processing of data intended to evaluate certain personal aspects relating to him, such as his performance at work, creditworthiness, reliability, conduct, etc." At the same time, article 15(2) states an exception: "a person may nevertheless be subjected to an automated individual decision if that decision is taken: (a) in the course of the entering into or performance of a contract, provided the request for the entering into or the performance of the contract, lodged by the data subject, has been satisfied or that there are suitable measures to safeguard his legitimate interests, such as arrangements allowing him to put his point of view; or (b) is authorized by a law which also lays down measures to safeguard the data subject's legitimate interests".

In the light of Article 15 of the DPD, it is relevant whether the processing is meant to evaluate a certain aspect of the person's behavior, character or identity on which a decision can be based. A decision based on a profile can comply with the law, but a natural person has to be involved in the process. To sum up, Article 15 does not take the form of a direct prohibition on a particular type of decision-making; rather, it directs each EU Member State to confer on persons a right to prevent them from being subjected to purely automated decisions in general.[68]

The directive proved unable to provide for sufficient protection in a fast-developing information society. In response to the technological developments of the past decades, the European Commission released in January 2012 a draft General Data Protection Regulation (GDPR) and a Data Protection Directive in the law enforcement context.

The GDPR contains one Article, Article no. 20, which concerns the data subject's right not to be subject to a measure based on profiling. It represents an evolution, with modifications and additional safeguards, of Article 15(1) and takes account of the Council of Europe's recommendation on profiling (Recommendation CM/Rec(2010)13). Compared to article 15, Article 20 better defines the right of a person not to be subject to a measure that is based solely on automated processing[69] and in particular clarifies that profiling cannot be based only on sensitive types of data (e.g. race or ethnic origin, religion, political opinion or sexual orientation), which would carry a too strong risk of discrimination on the basis of a prohibited ground.[70] Moreover it allows profiling in certain cases, but compared to article 15, the rules are stricter. Profiling is allowed when: (a) it is required for contracts, and

[68] Bygrave, Lee A., *Data protection law: Approaching its rationale, logic and limits* (The Hague: Kluwer Law International, 2002), 3.

[69] Article 20 par. 1: "Every natural person shall have the right not to be subject to a measure which produces legal effects concerning this natural person or significantly affects this natural person, and which is based solely on automated processing intended to evaluate certain personal aspects relating to this natural person or to analyse or predict in particular the natural person's performance at work, economic situation, location, health, personal preferences, reliability or behaviour."

[70] Article 20 par. 3: "Automated processing of personal data intended to evaluate certain personal aspects relating to a natural person shall not be based solely on the special categories of personal data referred to in Article 9".

the data subject has the right to request a human intervention; (b) it is permitted by law; or (c) under certain conditions, the data subject gives a free, explicit and informed consent.[71]

The novelty of this regulation is the provision contained in the fourth paragraph, which obliges data controllers to provide 'information as to the existence of processing" for an automated decision and about "the envisaged effects of such processing on the data subject".[72] As underlined in the advice paper released by Article 29 WP in May 2013[73] the GDPR does not include a definition of profiling. Blank spots like this prove that there is still a lot of work to do grasping profiling to enable an adequate regulation.

Another important aspect of learning more about profiling, its impacts, and the need for its regulation is getting to know about the awareness, the attitudes, and the activities of those authorities who are dealing with data protection and privacy on a day-to-day basis. That is why the project PROFILING has conducted a survey, which will be introduced in the next section.

1.6 National Data Protection Authorities' (DPAs) Responses to Profiling Questionnaire

In its aim to collect and compare information in the issue of profiling and, in particular automated profiling, the project PROFILING has developed a questionnaire – partly based on input from DPAs of Romania, Germany and Italy, the

[71] Article 20 par. 2: "Subject to the other provisions of this Regulation, a person may be subjected to a measure of the kind referred to in paragraph 1 only if the processing:

(a) is carried out in the course of the entering into, or performance of, a contract, where the request for the entering into or the performance of the contract, lodged by the data subject, has been satisfied or where suitable measures to safeguard the data subject's legitimate interests have been adduced, such as the right to obtain human intervention; or
(b) is expressly authorized by a Union or Member State law which also lays down suitable measures to safeguard the data subject's legitimate interests; or
(c) is based on the data subject's consent, subject to the conditions laid down in Article 7 and to suitable safeguards."

[72] See for weaknesses and strengths of this provision Bert-Jaap Koops, "*On decision transparency, or how to enhance data protection after the computational turn*," in *Privacy, Due Process and the Computational Turn: The Philosophy of Law Meets the Philosophy of Technology*, ed. Mireille Hildebrandt and Katja de Vries (Abingdon, Routledge, 2013), 189–213 and Mireille Hildebrandt, "*The Dawn of a Critical Transparency Right for the Profiling Era*," in *Digital Enlightenment Yearbook 2012*, ed. Jacques Bus et al. (Amsterdam: IOS Press, 2012), 41–56.

[73] Advice paper on essential elements of a definition and a provision on profiling within the EU General Data Protection Regulation http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2013/20130513_advice-paper-on-profiling_en.pdf.

EDPS and the Council of Europe[74] – that was sent to the 28 European National Data Protection Authorities and Switzerland. The questionnaire aimed to gain an overview of the profiling landscape in European Member States, meaning: the current and future legal framework, the domains of application, the complaints and remedies procedures regarding the use of profiling techniques, the main risks and benefits for the fundamental rights and, finally, citizens' awareness on this topic.

Eighteen DPAs completed the questionnaire; three DPAs informed us that they would not be able to complete the questionnaire, mainly for reasons of lack of resources (but two provided some information related to the questionnaire); the other eight DPAs did not respond.[75] We started compiling and analyzing the answers of the 18 DPAs and the first findings of the profiling questionnaire were presented at CPDP in January 2014. Here, we present a more elaborate first analysis of the survey results.

1.6.1 Findings

1.6.1.1 Legal Aspects

Even if the understanding of the meaning of automated profiling varies among countries, it seems the DPAs agree in three principal characteristics of profiling:

- It is based on a collection, storage and/or analysis of different kind of data;
- and on automated processing using electronic means;
- with an objective of prediction or analysis of personal aspects or personality and/or the creation of profile.

Additionally, a fourth key aspect for some DPAs is that the profiling results in legal consequences for the data subject.

Fifteen out of eighteen DPAs express the need of a legal definition of profiling in order to clarify the definition and conditions it can be used. Three DPAs (Hungarian, Swedish and British) are not in favor of a definition by law because it would create misinterpretation and it would be difficult to provide an exhaustive definition including every imaginable profiling situation. All along the questionnaire, the UK DPA explains it might be better to see profiling as another form of personal data

[74] We thank the Italian, Romanian and German DPAs, the EDPS and the Council of Europe for their feedback to our pre-test questionnaire.

[75] Within 2 months we received the questionnaire completed by 18 DPAs: Austria, Bulgaria, Croatia, Estonia, Finland, Germany, Greece, Hungary, Ireland, Italy, Lithuania, Malta, Romania, Slovakia, Slovenia, Sweden, Switzerland, and United Kingdom. Three DPAs informed us that they would not be able to complete the questionnaire, mainly because of lack of resources: Denmark, Luxembourg and Netherlands. However, DPAs from Luxembourg and Netherlands provided some information related to the questionnaire. Eight DPAs did not respond: Belgium, Cyprus, Czech Republic, France, Latvia, Poland, Portugal and Spain.

processing which should be regulated within the normal data protection framework and should be treated as just one variant of data processing.

The two main risks of profiling techniques mentioned by DPAs are the challenge posed to individuals' liberties and fundamental rights at large (privacy and data protection, self-determination, dignity, personal integrity, personality, free speech and movement), and the lack of transparency and awareness about the existence of profiling. On the other hand, some DPAs also state that profiling can be a useful tool for tailored commercial services.

All DPAs (except Estonia) agree that profiling is a challenging area to be regulated. And a majority (10/18) agrees that all steps[76] should be subject to strict regulation both at EU and national level. It is important to notice that for the Greek and Italian DPAs, profiling should be considered and regulated as a whole process not in different stages.

All the European Union countries answering (except Greece) have transposed Article 15 of the Directive 95/46/EC.[77] Switzerland is not bound to the Directive but its national Data Protection Act includes a definition of profiling. In contrast, no country has implemented Recommendation (2010)13 of the Council of Europe on profiling. Thirteen DPAs out of seventeen have directly or indirectly implemented Article 7 of the Decision 2008/977/JHA of the Council Framework on individual automated decision in the context of police and judicial cooperation in criminal matters through a specific Law or Act.

Apart from national provisions transposing Article 15 of the Directive 95/46/EC, only two countries (Germany and Italy[78]) have specific legal provisions on automated profiling in their legal framework.

One question inquired whether DPAs have written internal guiding policy or public policy addressing data controllers on the implementation of Article 15 and 12 of Directive 95/46/EC with regard to automated decision based on profiling.

[76] As defined by the Council of Europe, mainly (1) collection and storage of data, (2) correlation and analysis of data and (3) practical application of profiles.

[77] According to article 15(1): "every person has the right not to be subject to a decision which produces legal effects concerning him or significantly affects him and which is based solely on automated processing of data intended to evaluate certain personal aspects relating to him, such as his performance at work, creditworthiness, reliability, conduct, etc." At the same time, article 15 (2) states an exception: "a person may nevertheless be subjected to an automated individual decision if that decision is taken: (a) in the course of the entering into or performance of a contract, provided the request for the entering into or the performance of the contract, lodged by the data subject, has been satisfied or that there are suitable measures to safeguard his legitimate interests, such as arrangements allowing him to put his point of view; or (b) is authorized by a law which also lays down measures to safeguard the data subject's legitimate interests".

[78] Profiling is envisaged in the German Telemedia Act for the purposes of advertising, market research or in order to design the telemedia in a needs-based manner; in Italy, legal provisions on the assessment of income tax provide some type of profiling.

The questionnaire reveals that there are only few DPAs that have written policies[79] or have taken decisions[80] (4/18) on the implementation of those Articles 15 and 12. However, five[81] mentioned other policies related to them. It appears that those policies produced by DPAs are mostly addressed to data subjects' awareness and explain how to assert their rights rather than to DPA employees or to data controllers in order to clarify how to carry out the profiling.

Asked what are the main aspects that are important to be included in the General Data Protection Regulation (GDPR), first and foremost European DPAs call for a precise and broad definition of profiling and for adequate safeguards for individuals.

On the present draft of Article 20 of GDPR, eight DPAs estimate that it must be improved, while five support the new Article in whole or with some improvements. The major identified weaknesses of this Article concern the scope of the article, which should be broader and cover the entire processing of personal data, not only the result of the processing; some unclear terms that are dangerous for legal certainty (such as "legal effects" and "significantly affects" in the first paragraph and "suitable measures" or "safeguards" in the second paragraph); and the future use of sensitive data, which is unclear too. But they recognize that the fourth paragraph on data controller obligations is an improvement.

Nine DPAs out of twelve consider the Amendments from the European Parliament[82] as beneficial for establishing the final version of the Regulation (broader scope, clarifying the transparency obligations of data controllers, and hence improving data subjects' rights, and banning the use of sensitive data), but three do not support the recommendation of the report. Eight DPAs out of thirteen agree with

[79] Finland have a Guide on the processing of personal data in context of direct marketing and a Guide on a data subject's right of accede to his/her data which serve as official guidance to all); UK have Guides on subject access rights.

[80] Austria Data Protection Commission took nine decisions which may serve as guideline of their activities, available online at: http://www.ris.bka.gv.at/Dsk/; Italian DPA issued several decisions on profiling, for example on loyalty cards, on customer profiling as carried out by telecom operators, in employment sector and in respect of interactive TV.

[81] Hungarian former commissioner for data protection and freedom of information issued a report, in cooperation with the commissioner for ethnic and minority rights, on the processing of data relating to ethnic origin; Irish DPA provides general information and advice on the right of access of data subjects to their personal data, but not specifically tailored to the issue of automated profiling; Slovenia issued a couple of non-binding opinions on a credit worthiness system both to the data controller and to data subjects; Swedish DPA has published a leaflet on Article 12 that contains information about which public and private actors that process personal data and on how to proceed to exercise the right of access to personal data; Swiss DPA has provided guidance on subject access rights.

[82] Committee on Civil Liberties, Justice and Home Affairs of the European Parliament. Draft report on the proposal for a regulation of the European Parliament and of the Council on the protection of individual with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). 17/12/2012. Available online at: http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/pr/922/922387/922387en.pdf.

the three main arguments of the EDPS[83] supporting Article 20, especially the recommendation to restore the right for individuals to submit their point of view, but five out of thirteen are in favour of a more far-reaching Regulation on profiling. The Advice paper of the Article 29 Working Party[84] which proposes a definition of profiling[85] and provides several suggestions[86] on how to improve article 20 of the GDPR is approved by all the answering DPAs excepting Ireland, which prefers the proposal version.

Concerning Article 9 of the proposed Directive on Data Protection in the Law enforcement sector (COM(2012)10 final), five DPAs[87] support the current version or do not have any comment or serious concern about it. Three DPAs have a mixed opinion because even if they consider Article 9 as sufficient, they still have some hesitation: the Italian DPA recognizes the modification of "decisions" by "measures" as an improvement but would open the scope to "sensitive data which may also be generated by profiling and not only included in such activity" and would prefer reference to "personal data" rather than to "data"; the Maltese DPA suggests that "more specific guidance could be necessary on the application of this article when this is incorporated under national law"; and the Romanian DPA recommends the adoption of "legislative acts regulating the use of profiles in order to avoid the excessive collection of data" and the inclusion of "additional safeguards in order to protect the data subjects' rights, similarly with those provided by article 20 of the draft Regulation". Three DPAs share the opinion that Article 9 is not sufficiently protective: the Austrian and Irish DPAs do not approve the addition of "solely" in the second paragraph (see explanation above); the Finnish DPA asks for sufficient safeguards and ensure the purpose limitation principle. Regarding the Greek answer, the DPA considers that "Whereas the corresponding in the Regulation article seems as the EDPS mentions in its Opinion to build upon the existing art. 15 of the

[83] Opinion of the European Data Protection Supervisor on the data protection reform package. 7/03/2012.

[84] Article 29 Data Protection Working Party. Advice paper on essential elements of a definition and a provision on profiling within the EU General Data Protection Regulation. 13/05/2013.

[85] The definition proposed states that: "Profiling means any form of automated processing of personal data, intended to analyse or predict the personality or certain personal aspects relating to a natural person, in particular the analysis and prediction of the person's health, economic situation, performance at work, personal preferences or interests, reliability or behaviour, location or movements".

[86] Main proposals for improvement concern the scope: "It [. . .] welcomes Rapporteur Albrecht's proposal to broaden the scope of Article 20 covering processing of personal data for the purpose of profiling or measures based on profiling. The Working Party regards this as a necessary step towards more legal certainty and more protection for individuals with respect to data processing in the context of profiling"; a greater transparency and control for data subjects; more responsibility and accountability of data controllers; a balanced approach to profiling and the role of EDPS.

[87] Bulgaria estimates there are good balances between individual rights and data controllers' activity and between the general prohibition for processing sensitive data and the exceptions); Hungary support the Article, Croatia, Slovakia and Sweden do not have any comments or objections.

Directive 95/46/EC and extends its scope, art. 9 of the proposed Directive essentially only reiterates the relevant art. 7 of the Council Framework Decision 2008/977/JHA. Moreover, the content of this article is inconsistent with the Regulation as (for example) it does not explicitly provide for the analysis and evaluation of behaviour, whilst the prohibition of a measure based on automated processing of personal data (profiling) is conditioned only on the producing "an adverse legal effect" and not "a legal effect' as cited in the Regulation. Additionally, the relevant subject rights are specifically (with regard to the profiling) detailed in the Regulation, while similar provisions are absent in the proposed Directive. In our opinion the provisions of the Directive need to be more in line with the equivalent ones of the Regulation".

1.6.1.2 Domains of Application

We listed a number of domains where profiling is likely to be used, inviting the DPAs to identify in which of them profiling applied in their country at the national level. Finance sector (credit rating, anti-money laundering) is the most incline to apply profiling (18 DPAs/18), followed by marketing (15/18), social media and web and behavioral advertising (13/18), criminal investigation and employment (11/18), intelligence, national security, counter-terrorism, healthcare domain (including insurance) (10/18) and border control (9/18). Education domain resorts to profiling in only five countries. Irish DPA underlines that profiling happen in "insurance quotation generally" and Bulgarian DPA also mentions domains which were not predetermined: "namely-sociological agencies" and "TV and radio programs rating research".

The compilation of answers reveals that the most challenged domain for the DPAs is marketing (10 DPAs out of 14) followed by finance – credit rating, anti-money laundering – (9/14), social media and Internet, behavioral advertising (7/14), employment (6/14), healthcare (5/14), criminal investigation (4/14) and, finally, border control and national security (3/14).

One question related to the existence of any national law/regulation on the collection of personal data and on the use of such database. Numerous countries have pass regulations, through their Data Protection Act or through specific regulations and even, through Code of conduct approved by the DPA (Bulgaria).

1.6.1.3 Fundamental Rights

The main fundamental rights and principles challenged by profiling are private life and data protection, freedom rights (such as human personality, self-determination, free development, freedom of expression and movement, portrait rights or personal autonomy) and respect of the principles of purpose limitation, proportionality and necessity. And the risk of infringement of citizens' right of the protection of their personal data is considered higher in the financial domain (mentioned by 14 DPAs out of 14).

Article 20 of Directive 95/46/EC envisages a "prior checking", means that DPA should examine processing operations likely to present specific risks data subjects' rights prior to the start thereof. We asked whether the DPA envisage any specific procedure to be carried out to assess possible cases of infringements of fundamental rights and freedoms in profiling processes. Only 9 DPAs[88] out of 18 answered they have this possibility. Nevertheless, among the DPAs which do not envisage a prior checking, the Finnish DPA pointed out that it can control codes of conduct draft by controllers, in Germany prior checks are carried out by the data protection officers of public authorities and of private companies and the Romanian DPA can perform a preliminary control before the start of certain processing operations which are likely to present special risks for the persons' rights and liberties.

Thinking about concrete cases of infringements, according to the DPAs, the fundamental rights or principles most challenged by profiling are the right to data protection, followed by the right to privacy, the right to non-discrimination, the right to transparency, the right to autonomy and self-determination, and the right to due process in the rank of mentions.

1.6.1.4 Procedure to Complaint

A general procedure for data subjects' to directly complain about a data protection violation to the DPA can be designed following national legislations: a request is submitted by the plaintiff to the DPA against an act or omission of the data controller violating the law or his/her rights. If the complaint is admissible, the DPA initiates an investigation and then pronounces a decision (which is generally not as powerful as a court decision) in order to correct the violation. The individual is generally kept informed on the developments and notified of the final decision. The reasons for complaining are numerous (complaints based on violation of data subject rights or data breach) and concern various domains, but principally occur in the marketing domain.

About half of the DPAs have already received a complaint on automated profiling. Fifteen DPAs out of eighteen mention having already received complaints through legal entities, institutions, associations, law firms, attorney, representative to natural persons, bodies, organizations, NGOs, Trade Unions, foundation or local and central public authorities. All the DPAs can also investigate data processing practices at their own initiative but only 7 out of 15 have already used this right.

Article 23 of the actual Directive on data protection invites Member States to provide a compensation for "any person who has suffered damage as a result of an unlawful processing operation or of any act incompatible with the national provisions". According to DPAs' answers, such compensation mechanisms

[88] Austria, Bulgaria (but only for sensitive data), Croatia (not explicitly mention in the Data Protection Act), Hungary (audit and impact assessment envisaged as a prior checking procedure), Italy, Malta, Slovakia, Slovenia, UK (prior checking is in the Data Protection Act but has never been enforced).

are usually envisaged in European countries.[89] If the national Data Protection Acts do not necessarily foresee such compensation, data subjects can resort to civil, penal or administrative procedures. In some countries there are also other entities able to take care of it, such as the Competition Authority or the Authority for Consumer Protection in Hungary. On the relevant court cases on automated profiling, only the Italian DPA mention that a case is currently pending before the Italian Supreme Court of Cassation regarding the case of profiling carried out by the National Printing Institution on its employees. The case originated from the challenging of a decision adopted by the Italian DPA on 21 July 2011.[90]

One question concerned the existence of a specific national training, instruction or guidance on profiling for the DPA officials. There are only three countries where DPA officials receive this kind of training. The Finnish DPA has issued a number of guidance (particularly on marketing practices), the Italian DPA has organized some internal seminars regarding the most controversial aspects of profiling and the Slovakian DPA performs training of its employees but not only in the area of profiling.

1.6.1.5 Awareness

Among a list of reasons likely to influence data subjects' decisions to submit a complaint in case of automated profiling that significantly affects them, DPAs principally mention the awareness of the legal effects of individual measures based on profiling (15/17), closely followed by the awareness of their fundamental rights, transparency of the profiling process and to be informed that a certain decision is (partly) based on profiling (14/17 for each). As a corollary, the main limitation for data subjects' understanding of profiling risks and implications according to the DPAs is considered to be a lack of knowledge of the existence of the profiling and of transparency over the processing.

[89] Austria (before a court but not in practice), Bulgaria (under civil law not in the Data Protection Act which foresee administrative penalties-fines/sanctions), Croatia (before a court of general jurisdiction), Estonia (no precision), Finland (before a district court in civil procedure), Germany (the DPA of the non-public sector can impose a fine and civil procedure also apply), Greece (under civil procedure), Hungary (through civil and other procedures), Ireland (no direct compensation before the DPA but possible through civil procedure), Italy (judicial authorities competence), Lithuania (civil court competence), Malta (civil court competence), Romania (court of Law competence), Slovakia (not under the DPA but through civil Court), Slovenia (the civil law give competence to Court and relevant Authorities), Sweden (the Data Protection Act envisage compensation but not specific to profiling), UK (court competence). Switzerland did not answer.

[90] Answer of the Italian DPA ('Garante'): "*On 21 June 2011, our DPA adopted a decision concerning the profiling carried out by the National Printing Institution on its employees, in particular as a result of the monitoring of the employees' activities on the Internet. In such decision our DPA prohibited the unlawful data processing operations which had been carried out, inter alia, without informing the data subjects and notifying the processing to the Garante (*http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1829641*).*"

DPAs use many ways to improve the awareness of the general public about their rights as regards data collected and used for profiling purposes: websites, written documentation (reports, guidelines, newsletter, leaflet…), internal and external seminars/conferences, media contributions, annual surveys and hotlines. Ten DPAs out of eighteen have already produced a report or study on the issue of profiling to increase data subjects' awareness. Finally, almost all DPAs think data subjects' awareness of automated profiling and its possible implications should be increased. In order to perform this aim, they suggest using numerous ways/tools and to involve private entities and consumer protection bodies.

1.7 Conclusions

The respect of fundamental rights and values is essential to guarantee democracy and the rule of law. But in a world where new technologies fundamentally change social relations and practices, it is not always clear what human rights and the rule of law actually mean, and how respect for human rights can be safeguarded. This paper has delivered an overview of the technological evolution and elaborated the socio-technological preconditions of profiling. It demonstrated how the new technological advances change social practices and how pose threats to fundamental rights and values of European societies when applied in various fields and contexts. Despite these critical implications, the DPA questionnaire highlights a lack of a common definition and of a mutual vision on how to deal with the challenges emerging from profiling.

The survey showed that national legal frameworks on automated profiling within the European Union and Switzerland look quite similar. Moreover, there is a sense of global coherence between the DPAs' points of view on the understanding of automated profiling, even if it is a new and fast-moving domain. Furthermore a majority of DPAs express the need for legal regulation. However, when discussing future regulation, discrepancies appear amongst the DPAs, both concerning Article 20 of the GDPR and Article 9 of the proposed Directive. Whereas one group supports the new proposal as is, the other group is calling for reinforcing its data protection measures. A full discussion is needed in order to better identify dangers associated with the use of automated profiling and to identify the importance given to fundamental rights protection, in particular data protection.

DPAs within the European Union and Switzerland have received only few complaints on profiling. This can be due to the novelty of the use of automated profiling, and also to a general lack of awareness by the citizenry. The awareness of the legal effects of individual measures based on profiling, and the awareness of citizens' fundamental rights and of profiling as a process are factors likely to influence data subjects' abilities to submit complaints in cases of automated profiling that significantly affect them. Our survey reveals that even though data subjects' awareness is an important and a highly worrisome issue for DPAs, there is a lack of guidance dedicated to profiling. Therefore, it is important for DPAs to provide complete and understandable information on the concept of profiling, its purposes and the potential risks and implications of this method.

To conclude, national data protection authorities state that profiling is a challenging and risky activity. They now need to take the necessary measures to improve the training of employees, make data controllers aware of their responsibilities; and in particular, enhance citizen awareness, for the lack of knowledge about profiling and the lack of transparency in information processing are the main limitations for data subjects' understanding of profiling's risks and implications.

The new issues posed by technological development challenge current and future regulation to adequately respond to matters related to self-determination especially regarding the problem of the general applicability of data protection to profiling and the efficiency of technical approaches such as anonymity and de-identification. It is paramount to enhance the critical thinking on the possibilities, as well as the limitations, of improving data protection in the current and future technological setting.

References

Anrig, Bernhard, Brown, Will and Gasson, Mark, "The Role of Algorithms in Profiling," in *Profiling the European Citizens. Cross-Disciplinary Perspectives*, edited by Mireille Hildebrandt and Serge Gutwirth, 65–87, Dordrecht: Springer, 2008.

Baskarada, Sasa and Koronios, Andy, "Data, Information, Knowledge, Wisdom (DIKW): A Semiotic Theoretical and Empirical Exploration of the Hierarchy and its Quality Dimension." *Australasian Journal of Information Systems*, Vol 18, No 1 (2013): 5–24.

Brakel, Rosamunde van and Paul de Hert. "Policing, surveillance and law in a pre-crime society: Understanding the consequences of technology based strategies." *Cahier Politiestudies* 20 (2011): 163–192.

Bygrave, Lee A. *Data protection law: Approaching its rationale, logic and limits*. The Hague: Kluwer Law International, 2002.

Calders, Toon and Žliobaitė Indrė. "Why Unbiased Computational Processes Can Lead to Discriminative Decision Procedures." In *Discrimination and Privacy in the Information Society. Data Mining and Profiling in Large Databases*, edited by Bart Custers et al., 43–57. Berlin: Springer, 2013.

Canhoto, Ana and Blackhouse, James, "General Description of Behavioural Profiling," in *Profiling the European Citizens. Cross-Disciplinary Perspectives*, edited by Mireille Hildebrandt and Serge Gutwirth, 47–63, Dordrecht: Springer, 2008.

Chang, LiWu, und Ira S. Moskowitz. "An Integrated Framework for Database Privacy Protection" In *Data and Application Security*, herausgegeben von BhavaniThuraisingham, Reind van de Riet, Klaus R. Dittrich, und ZahirTari, 161–72. IFIP International Federation for Information Processing 73. Springer US, 2001. http://link.springer.com/chapter/10.1007/0-306-47008-X_15.

Clarke, Roger, "Profiling: A Hidden Challenge to the Regulation of Data Surveillance". In *Journal of Law and Information Science* 4, 2 (1993): 403–419.

Degele, Nina, *Einführung in die Techniksoziologie*. Stuttgart: UTB, 2002.

Deleuze, Gilles. "Postskriptum über die Kontrollgesellschaften" In *Unterhandlungen 1972–1990*, Gilles Deleuze, 254–262. Frankfurt a.M.: Suhrkamp, 1992.

Deutscher Bundestag, "Automatisierte Strafverfolgung, Data Mining und sogenannte erweiterte Nutzung von Daten in polizeilichen Informationssystemen." *Drucksache 17/11582*, 22 November 2012, http://dip21.bundestag.de/dip21/btd/17/115/1711582.pdf, last accessed 26 March 2014.

Deutscher Bundestag, "Computergestützte Polizeitechnik bei Polizeibehörden." *Drucksache 17/8544 (neu)*, 06 Feb 2012, http://dipbt.bundestag.de/dip21/btd/17/085/1708544.pdf, last accessed 01 April 2014.

Finn, Rachel L, David Wright and Michael Friedewald. "Seven Types of Privacy." In *European Data Protection: Coming of Age*, edited by Serge Gutwirth et al., 3–32, Dordrecht: Springer, 2013.

Fraunhofer. IAIS, "*Big Data – Vorsprung durch Wissen. Innovationspotenzialanalyse*," http://www.bigdata.fraunhofer.de/content/dam/bigdata/de/documents/FraunhoferIAIS_Big-Data-Analyse_Doku.pdf, last accessed 01 April 2014.

Fuster, Gloria González, Gutwirth Serge, and Ellyne Erika. "Profiling in the European Union: A high-risk practice" *INEX Policy Brief* 10 (2010): 1–12.

Gellert, Raphael and Serge Gutwirth. "Beyond accountability, the return to privacy?" In *Managing Privacy through Accountability*, edited BY Daniel Guagnin et al., 261–284. Houndmills: Palgrave Macmillan, 2012.

Guagnin, Daniel et al., eds. *Managing Privacy Through Accountability*. Houndmills: Palgrave, 2012.

Gutwirth, Serge and Hildebrandt Mireille. "Some Caveats on Profiling." In *Data protection in a profiled world*, edited by Serge Gutwirth, Yves Poullet and Paul de Hert, 31–41. Dordrecht: Springer, 2010.

Gutwirth, Serge and Paul de Hert. "Regulating profiling in a Democratic Constitutional State." In *Profiling the European Citizens. Cross-Disciplinary Perspectives*, edited by Mireille Hildebrandt and Serge Gutwirth, 272–293 Dordrecht: Springer, 2008.

Hildebrandt, Mireille. "The Dawn of a Critical Transparency Right for the Profiling Era". In *Digital Enlightenment Yearbook 2012*, edited by Jacques Bus, Malcolm Crompton, Mireille Hildebrandt, George Metakides, 41–56. Amsterdam: IOS Press, 2012.

Hildebrandt, Mireille. "Defining profiling: a new type of knowledge?" In *Profiling the European Citizens. Cross-Disciplinary Perspectives*, edited by Mireille Hildebrandt and Serge Gutwirth, 17–47. Dordrecht: Springer, 2008.

Hildebrandt, Mireille. "Profiling and AML," in *The Future of Identity in the Information Society. Challenges and Opportunities*, edited by Rannenberg Kai, Denis Royer and André Deuker, 273–310. Heidelberg: Springer, 2009a.

Hildebrandt, Mireille. "Profiling: from Data to Knowledge. The challenges of a crucial technology." *DuD Datenschutz und Datensicherheit*, 30, 9 (2006): 548–552.

Hildebrandt, Mireille. "Technology and the End of Law." In *Facing the Limits of the Law*, edited by Erik Claes, Wouter Devroe and Bert Keirsbilck, 443–465. Heidelberg: Springer, 2009b.

Hildebrandt, Mireille. "Who is Profiling Who? Invisible Visibility." In *Reinventing Data Protection?*, edited by Serge Gutwirth et al., 239–252. Dordrecht: Springer, 2009c.

Hunko, Andre, *"Suchbewegungen zu Data Mining-Software gehen über gesetzlichen Auftrag des BKA hinaus,"* 17 March 2014, http://www.andrej-hunko.de/presse/1934-suchbewegungen-zu-data-mining-software-gehen-ueber-gesetzlichen-auftrag-des-bka-hinaus, last accessed 26 March 2014.

Koops, Bert-Jaap (2013). "On decision transparency, or how to enhance data protection after the computational turn." In *Privacy, Due Process and the Computational Turn: The Philosophy of Law Meets the Philosophy of Technology*, edited by Mireille Hildebrandt and Katja de Vries, 189–213. Abingdon: Routledge.

Koops, Bert-Jaap. "Technology and the Crime Society: Rethinking Legal Protection." *Law, Innovation & Technology*, 1, 1 (2009): 93–124.

Latour, Bruno "Technology is Society Made Durable." In *A Sociology of Monsters: Essays on Power, Technology and Domination*, edited by John Law, 103–131. London: Routledge, 1991.

Lianos, Michaelis and Mary Douglas. "Dangerization and the End of Deviance: The Institutional Environment." *British Journal of Criminology* 40, 2 (2000): 261–278.

Lyon, David "Surveillance as Social Sorting. Computer Codes and Mobile Bodies," in *Surveillance As Social Sorting: Privacy, Risk, and Digital Discrimination*, edited by David Lyon, 13–31. City: Psychology Press, 2003.

Marx, Gary and Reichman Nancy. “Routinizing the Discovery of Secrets: Computers as Informants”. In *American Behavioral Scientist*, 27, 4 (1984): 423–452.

Monahan, Torin “Surveillance as Governance: Social Inequality and the Pursuit of Democratic Surveillance.” *Surveillance and Democracy issue (*2010): 91–110.

O‘Malley, Pat. “Risk, power and crime prevention.” *Economy and Society* 21, 3 (1992): 252–275.

Ohm, Paul. “Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization,” *UCLA Law Review* 57 (2010): 1701–1777.

Özden Melik “The Right to non-discrimination”, in *Series of the Human Rights Programme of the CETIM*, 2011.

Pedreschi, Dino, Ruggieri Salvatore, Turini Franco. “The Discovery of Discrimination.” In *Discrimination and Privacy in the Information Society. Data Mining and Profiling in Large Databases*, edited by Bart Custers et al., 91–108. Berlin: Springer, 2013.

Polakiewiecz, Jörg. “Profiling – The Council of Europe’s Contribution.” In *European Data Protection: Coming of Age*, edited by Serge Gutwirth et al., 367–377, Dordrecht: Springer, 2013.

Rodotà, Stefano. “Data Protection as a Fundamental Right.” In *Reinventing Data Protection?*, edited by Serge Gutwirth et al., 77–82. Dordrecht: Springer, 2009.

Romei, Andrea and Ruggieri Salvatore. “Discrimination Data Analysis: A Multi-disciplinary Bibliography.” In *Discrimination and Privacy in the Information Society. Data Mining and Profiling in Large Databases*, edited by Bart Custers et al., 109–135. Berlin: Springer, 2013.

Roosendaal, Arnold. *Digital Personae and Profiles in Law. Protecting Individuals’ Rights in Online Contexts*, Oisterwijk: Wolf Legal Publishers.

Rouvroy, Antoinette and Yves Poullet. “The right to informational self-determination and the value of self-development. Reassessing the importance of privacy for democracy.” In *Reinventing Data Protection?*, edited by Serge Gutwirth et al., 45–76. Dordrecht: Springer, 2009.

Sackmann, Stefan, Strüker, Jens, and Accorsi, “Personalization in Privacy-aware Highly Dynamic Systems”. *Commun. ACM* 49, Nr. 9 (September 2006): 32–38. doi:10.1145/1151030.1151052.

Scharff, Thomas. “Erfassen und Erschrecken. Funktionen des Prozeßschriftguts der kirchlichen Inquisition in Italien im 13. Und frühen 14. Jahrhundert.” In *Als die Welt in die Akten kam. Prozeßschriftgut im europäischen Mittelalter*, edited by Susanne Lepsius and Thomas Wetzstein, 255–274. Frankfurt a.M.: Vittorio Klostermann, 2008.

Schermer, Bart. “Risks of profiling and the limits of data protection law.” In *Discrimination and Privacy in the Information Society. Data Mining and Profiling in Large Databases*, edited by Bart Custers et al., 137–154. Berlin: Springer, 2013.

Solove, Daniel J. “I’ve Got Nothing to Hide’ and Other Misunderstandings of Privacy.” *San Diego Law Review*, 44 (2007): 745–772.

Solove, Daniel J. *Digital Person: Technology and Privacy in the Information Age*. New York: New York University Press, 2004.

Streibich, Karl-Heinz, “Big Smart Data. MehrwertfürUnternehmen”, (paper presented at the Big Data Days, Berlin, Germany, November 11–12, 2013).

Susanne Krasmann, “Der Präventionsstaat im Einvernehmen. Wie Sichtbarkeitsregime stillschweigend Akzeptanz produzieren.” In *Sichtbarkeitsregime: Überwachung, Sicherheit und Privatheit im 21. Jahrhundert*, edited by Leon Hempel, Susanne Krasmann and Ulrich Bröckling, 53–70. Wiesbaden: VS Verlag, 2010.

Trudel, Pierre. “Privacy Protection on the Internet: Risk Management and Networked Normativity.” In *Reinventing Data Protection?*, edited by Serge Gutwirth et al., 317–334. Dordrecht: Springer, 2009.

Vedder, Anton. “KDD: The challenge to individualism.” *Ethics and Information Technology* (1999): 275–281.

Verykios, Vassilios S. et al., “State-of-the-art in Privacy Preserving Data Mining”. *SIGMOD Rec.* 33, Nr. 1 (März 2004): 50–57. doi:10.1145/974121.974131.

Zakaria, Fareed. “The rise of illiberal democracy.” *Foreign Affairs*, 76, 6 (1197): 22–43.

Zarsky, Tal Z., “Mine Your Own Business!’: Making The Case For The Implications Of The Data Mining Of Personal Information in the Forum of Public Opinion.” *Yale Journal of Law & Technology* 5 (2002–2003): 1–56.

Chapter 2
On-line Behavioral Tracking: What May Change After the Legal Reform on Personal Data Protection

Georgia Skouma and Laura Léonard

Abstract On-line tracking has gained over the last years a new dimension: it has become an intrinsic part of our Internet-driven society. It touches all levels and types of industries. Consequently, more and more individuals become the target of this trend as routinely users of the internet. On-line tracking techniques are subject to the European personal data protection rules currently in force, insofar as they process information that identifies or may potentially identify a natural person. Nevertheless, the unprecedented threats that such techniques entail to privacy must have been a core motive opening the way towards the revision of the privacy regulations applicable today. New requirements and concepts strengthening the rights of data subjects and the obligations of data controllers or processors are set forth in the current draft of the new Regulation (currently under discussion within the EU institutions). This envisaged legal reform may however prove to be insufficient unless, at the same time, effective measures are adopted to help both on-line users, especially those of young age, and the companies implementing on-line tracking tools in order to change their approach to privacy.

With the exponential growth of "smart" technologies, new forms of tracking individuals' behavior, habits, and personality have emerged. Amongst those, the tracking of users while they are interacting over the Internet (on-line tracking), has proved its added-value primarily to marketing and advertising companies, but also other industries which increasingly use those smart techniques next to other intelligent "customer relationship management" (CRM) tools.

The opinions expressed in this article reflect the personal views of the authors and do not engage in any way whatsoever the company with whom they are working.

G. Skouma (✉) • L. Léonard
Department of Security and Privacy, Deloitte Bedrijfsrevisoren/Réviseurs d'Entreprises, Diegem, Belgium
e-mail: gskouma@deloitte.com; lauleonard@deloitte.com

S. Gutwirth et al. (eds.), *Reforming European Data Protection Law*,
Law, Governance and Technology Series 20, DOI 10.1007/978-94-017-9385-8_2

The majority of on-line tracking technologies today is based on cookies; by using cookies as the backbone, the designers of on-line tracking tools have developed other smart applications. On-line tracking applications of the latest technology combine users' data through observation tags, analyze them using algorithms, and then compare them with a mass of other data that have been collected by many other users. The purpose of the data analysis and mapping to the "stock" of data already collected is to adduce some conclusions about the interests, marketing and buying habits of the tracked individuals. Other on-line tracking smart solutions dig into the traces website users leave on social networking tools, combine them with data collected off-line, and make up with sometimes (not) so great accuracy the profile of an individual.

All above on-line tracking techniques are already subject to the European personal data protection rules underpinned in the current Data Protection Directive (95/46/EC) insofar as they process information that identifies or may potentially identify a natural person. The basic personal data protection requirements stemming from the principles of purpose limitation, data minimization, proportionality, transparency, data destruction—to mention only some of those—are undoubtedly of great relevance here. Nevertheless, at the time the Directive was enacted, the EU legislator could not predict the massive use of on-line tracking tools we are all subject to nowadays as routine internet users. This is probably one of the reasons why the draft Regulation on personal data protection ("Regulation"), that is ought to replace the aforementioned Directive, reserves in its current wording very specific phrasing around users' monitoring and profiling. First, it seems that the risks associated with online activity have been one of the major incentives to suggest the revision of the existing regulatory framework of personal data protection (Recital 7 of Regulation). Second, a number of requirements set forth in the Regulation strengthen and specify more practically legal rules that are found back in the current legislative framework. This is the case notably with the consent, transparency, and notice requirements. Finally, yet most importantly, a few new concepts formally introduced by the Regulation for the first time, such as the privacy by design principle or the right to be forgotten (or right to erasure) will have a major impact (on condition that they are effectively implemented) on the designers of the on-line tracking solutions, as well as on the companies implementing them.

Yet if the Regulation is adopted with the wording proposed today (or stricter one), will this ensure that the overarching privacy right of the on-line users and the rights resulting from it will be better protected? Undoubtedly this will not be the case if the user's mentality around the "on-line activity" does not change. Users, especially those of young age, many times truly addicted to the network, must constantly reminded of the huge potential that their data represent for marketing companies but also for any other organization wishing to learn about them (headhunters, employers, social networks, press and media, police, law enforcement agencies and so on). Moreover, actions to incentivize on-line users and the implementers of on-line tracking technologies to demand *proven controls* from the designers and vendors of such tools that they adequately safeguard users' privacy may be an addition to ensure better and effective protection. Regulators, standards-setting bodies, and public interest organizations are some of the categories of market stakeholders who could efficiently drive and monitor users' and implementers' awareness, education, and if needed, meaningful enforcement.

2.1 On-line Behavioral Tracking

2.1.1 Definition and Today's Trends

If on-line behavioral tracking has its roots in the marketing industry,[1] it has gained over the years and due to the emergence of smart technologies, a new dimension: currently, behavioral tracking has become an intrinsic part of our internet-driven society. From a marketing trend (known as on-line *behavioral advertising*), it has rapidly become a general *industry trend* with a deep impact on our everyday activities; it crosses the borders of our privacy. In that sense, the citizen of our Information Society today is tracked constantly on the street (camera surveillance), in car (radars and geo-localization devices), at the workplace (badging, biometrics, monitoring of PC and phone) or during the majority of his other activities (travelling, shopping – RFID –, leisure, and so on).

Amongst all these methods of tracking individuals' behavior, the on-line behavioral tracking represents an important part, as it happens easily and is based on common technological tools an individual is carrying (such as a laptop, a smartphone, an iPad) and which provide connection to *the Internet*. In other words, on-line tracking consists of recording and collecting data linked to an individual visiting the Internet through such tools over a period of time in order to gain information on this individual.[2] The information collected forms a source of knowledge linked to the person in question. The knowledge involved in tracking is not empirical or technical. On-line tracking has actually been turning into a real science (part of marketing "intelligence") in which professionals are developing advanced models and patents to optimize the analysis over the data tracked and provide "unique" insights. The on-line behavioral tracking enables the collection of many and diverse data about a person, ranging from merely identification details (such as a user name or a subscriber's name) or the means connecting the person to the internet (IP address), to information which could reveal a lot about an individual's personality, hobbies, interests, shopping habits, favorite activities and so on. Many

[1] Matthew S. Kirsch, *Do-Not-Track: Revising the EU's Data Protection Framework to Require Meaningful Consent for Behavioral Advertising*, (XVIII RICH. J.L. TECH. 2) available at http://jolt.richmond.edu/v18i1/article2.pdf.

[2] M. Hildebrandt, *Profiling: from data to knowledge* (DuD: Datenschutz und Datensicherheit 30, 2006 9), 548-549;

P. Eckersley, *What does the "Track" in Do Not Track Mean?* (Electronic Frontier Foundation, 19 February 2011) available at https://www.eff.org/deeplinks/2011/02/what-does-track-do-not-track-mean, 548-549.

times, the data tracked through the on-line behavioral techniques explained below are even sensitive data (revealing a person's sexual orientation or philosophical beliefs, for example). If the collection of the data is the first dimension of the on-line behavioral tracking, the second is the "mapping together" or correlation of these data in order to adduce meaningful conclusions about such individual (e.g. about his habits, interests, etc.) or in order to situate him in a particular category (e.g., the type of "buyer" he is). A third dimension is the assembling of data and the comparison of this set of data with other matched data referring to other persons or categories of persons with a view to creating the user's profile.

Examples of online behavioral tracking are broadly discussed in literature and refer to real examples from ordinary web users while surfing on the internet. Imagine yourself visiting an e-commerce website selling clothes. You are specifically searching for shoes. The day after, you visit again the same e-commerce website and the website proposes you a selection of articles you may like. The selection is only composed of pairs of shoes. Even though you did not purchase the product at the end, the site recorded your preferences and adapted the content it to your interests. The majority of the stated examples, as this one, discuss on-line behavioral tracking as used by the marketing and sales industry and, more in particular, in an advertising context.[3] Yet, some types of on-line tracking technologies may target citizens for other reasons, such as in order to detect a person's political affiliation and societal activities, work history, social networking activity, religious convictions, and other aspects of his private life and personality. In the same vein, the reasons for performing online behavioral tracking vary from merely lucrative and consumption-driven (advertising) reasons to political motives or reasons related to public and state safety, public security and the like. Thus, targeted advertising online is just a facet of tracking and probably the most widespread one, but not necessarily the only one.

2.1.2 Techniques of Online Tracking

On-line tracking techniques and intelligent "searching" over the internet evolve as fast as "smart" automated technology evolves in general. On the other hand, the research community, with sometimes contributions of industry, have been increasing their efforts to promote technological solutions that enable citizens to better control their data on-line.[4] Moreover, regulators, public interest stakeholders and the EU

[3] Advertising can be defined as the activity that consists of attracting potential customers to purchase or use a specific product by using media or other means. Clearly, advertising includes a lucrative purpose. On the contrary, tracking is more general and does not necessarily include a lucrative element.

[4] See in this regard the results of two research projects funded through successive Framework Programs of the European Commission, namely the PRIME and PrimeLife projects (www.primelife.ercim.eu). Both projects had as objectives to show how privacy technologies can enable

legislative bodies seem eager to enhancing users' awareness around the so-called Privacy Enhancing Technologies (PETs).[5]

Which are however the most common "business intelligent" techniques and tools nowadays which collect the human traces on the internet? The predominant technological means used remains the cookie.

The section below discusses the role that cookies could play in on-line tracking, as well as a number of other tools and market trends that systematically or inadvertently can scrutinize individuals and their behavior on-line. The purpose of the section is not to provide an exhaustive list of such techniques but to stress to the reader how tools that represent today "widely accepted" business practices may hide, each one to a less or greater extent, a threat to privacy.

2.1.2.1 On-line Scrutiny Through Cookies: Are They Always a Threat to Privacy?

A cookie is a *"piece of text stored by a user's web browser and transmitted as part of an HTTP request"*.[6] It contains bits of information and it is set by a web server.

A first distinction that can be made between the different types of cookies used is between "first party" and "third party" cookies. First-party cookies are

citizens to execute their legal rights to control personal information in on-line transactions. The main objective of these projects was to bring sustainable privacy and identity management to future networks and services. It is noteworthy that well-known software vendors were members of the research consortium having conducted this project. Some more information about the PETs and their added-value for business, see: Privacy-enhancing technologies for the Internet. Ian Goldberg, David Wagner, Eric Brewer.

http://www.cs.berkeley.edu/~daw/papers/privacy-compcon97-www/privacy-html.html; Study on the economic benefits of privacy-enhancing technologies (PETs), Final Report to The European Commission DG Justice, Freedom and Security, Prepared by London Economics, July 2010 at http://ec.europa.eu/justice/policies/privacy/docs/studies/final_report_pets_16_07_10_en.pdf (the article contains relevant examples of PETs and a business survey regarding the use of PETs; Privacy Enhancing Technology. Privacy Enhancing Technology. Guidelines and Testing Methodology, W3C/QA Position Paper, Tara M. Swaminatha at http://www.w3.org/2001/01/qa-ws/pp/tara-swaminatha-cigital.html. The article gives an introduction on the fact that the market has seen an increasing flood of privacy enhancing products.

[5] The European Commission seems to accept the definition of PETs as provided in the EC-funded PISA project, being "a coherent system of ICT measures that protects privacy by eliminating or reducing personal data or by preventing unnecessary and/or undesired processing of personal data, all without losing the functionality of the information system", see Communication from the Commission to the European Parliament and the Council on promoting data protection by privacy-enhancing technologies. COM(2007) 228 final. According to the same Communication, examples of PETs include encryption tools preventing tracking of the data transferred; cookie-cutters blocking cookies placed on user's PC; the platform for Privacy Preferences (P3P) allowing users to analyse privacy policies and compare them to their preferences.

[6] ENISA, *Privacy considerations of online behavioural tracking,* (October 2012) available at http://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/privacy-considerations-of-online-behavioural-tracking, 6.

implemented by companies on their own websites enabling such companies to interact directly with the users who visit their sites. On the contrary, when a company enables other third parties to track the users visiting its website, for example, by placing advertisements of third party vendors, then we talk about "third party" cookies.[7] Companies implementing first party cookies can control better the types of information that is stored on the cookies and decide on their own how to use the information collected through their own cookies. On the contrary, the companies accepting cookies of other vendors on their websites often waive any responsibility relating to how the companies having placed the cookies will treat the information collected through such cookies. It is obvious that third party cookies represent a greater risk to privacy compared to first party cookies since in the first case it becomes more complicated for users to keep an effective control over their data.

A second notable differentiator amongst the cookies used on vendors' websites is the time of tracking. It is generally accepted that session cookies are less offensive to individual's privacy as they capture information on the website instantly and they are automatically deleted when closing the browser. Accordingly, the session cookies store information when the user is interacting with the website. The information stored on session cookies are typically navigation choices and preferences of the users. The law and market practices tend to consider session cookies as useful for a good navigation along a website.[8]

Contrary to session cookies, the persistent cookies remain when closing the browser and need to be deleted by the user or with a planned cleaning set up in the browser settings. The persistent cookies aim in general to collect identifying information, interests of the users navigating on a website, preferences and authentication information. They allow the connection between pragmatic information and a specific user, and they are reactivated *by design* when the user comes back to the website.

For these reasons, persistent cookies raise serious concerns from a privacy point of view. The knowledge accumulated within the cookies resulting from the users' navigation and clicking on the URL of different webpages, targets users with personalized advertisements, tailored to the purported preferences and pattern of the behavior the user expressed on-line.

[7] ENISA, *Privacy considerations of online behavioural tracking,* (October 2012) available at http://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/privacy-considerations-of-online-behavioural-tracking, 3.

[8] The e-Privacy Directive states that the obligation of confidentiality of the communications "shall not prevent any technical storage or access for the sole purpose of carrying out or facilitating the transmission of a communication over an electronic communications network, or as strictly necessary in order to provide an information society service explicitly requested by the subscriber or user" (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, as amended by Directive 2009/136, art. 5 point 3).

To be noted that, in most cases, the way in which the company defines the parameters of information collection through cookies is a decisive factor for qualifying the cookie as really "privacy intrusive" or not. An example could help us illustrate this observation. Let us imagine a company using session cookies that instantly capture very basic details identifying an individual (e.g. the user name and password the user has used for registration on the website). Concurrently, the said company has foreseen that the data will be stored on such cookies in an encrypted form. On the opposite to that, another company displays on its website third party cookies that collect not only basic identifying information about a user but also more sensitive information, such as the number of the user's credit card or the product purchases he effected on the site. In both cases, the same technology is used (cookies), but the way in which cookies are designed to capture information is different.

2.1.2.2 Javascript

When navigating on the Internet, many Javascript files are downloaded. These files can be used for first-party tracking and the information collected will be sent back to the servers.[9] In terms of level of threat to privacy, Javascript files are comparable to first-party cookies. In addition, users can take action in order to block the storage of data collected by Javascript files.

2.1.2.3 Stateless Tracking

Without using cookies or other tracking technologies, web browser identification can be used as a tracking method.[10] Indeed, web browsers provide information such as fonts, screen resolution, equipment used and the like, that may allow the recognition of a web browser amongst others. This tracking method, also called Browser Fingerprinting, is more difficult to block as it is particularly difficult to detect.[11]

[9] ENISA, *Privacy considerations of online behavioural tracking,* (October 2012) available at http://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/privacy-considerations-of-online-behavioural-tracking, 6.

[10] P. Eckersley, *How unique is your web browser?* (Privacy Enhancing Technologies, Springer Berlin Heidelberg, 2010) in *Consumer Privacy Law 2: Data Collection, Profiling and Targeting* (July 16, 2009, Law And The Internet, L. Edwards & C. Waelde, eds., Hart Publishing, 2009) available at https://panopticlick.eff.org/browser-uniqueness.pdf.

[11] P. Eckersley, *How unique is your web browser?* (Privacy Enhancing Technologies, Springer Berlin Heidelberg, 2010) in *Consumer Privacy Law 2: Data Collection, Profiling and Targeting* (July 16, 2009, Law And The Internet, L. Edwards & C. Waelde, eds., Hart Publishing, 2009) available at https://panopticlick.eff.org/browser-uniqueness.pdf.

2.1.2.4 Supercookies and Evercookies

Over the years, users have taken into consideration the threats associated to their privacy by tracking techniques when navigating on a website. They have also been offered new applications that are designed to block cookies and delete them on a regular basis. Therefore, new means of tracking have emerged. Amongst these, new types of cookies have appeared: supercookies and evervookies.[12],[13],[14]

Supercookies, also called Flash cookies are robust tracking mechanisms placed on a user's computer.[15] Flash cookies are often linked and placed by Adobe Flash plug-in on websites. These cookies collect personal or technical information. As in other types of cookies, when supercookies are installed no specific notification is provided to users and they do not expire. What makes supercookies more "privacy-evasive" than the aforementioned other types of cookies is that, as they are located outside the browser's control, it makes it more difficult for the user to delete and control them.[16]

Evercookies is Javascript API that produces very powerful and persistent cookies, enabling the storage of cookie data in several types of storage mechanisms in the local browser.[17] Because of their particular storage, Evercookies are therefore meant to remain, even when the standard and Flash cookies have been removed from the browser.[18] Indeed, because they remain even after the user has deleted them, they clearly conflict with user's freedom and autonomy if the latter would wish to delete them.

2.1.2.5 Location Tracking

The geo-location plug-in installed on most of the popular browser and now installed on every smartphone, can be used as a tracking tool. On the basis of the user's consent, the browser shares information such as the IP address, the MAC address,

[12] ENISA, *Privacy considerations of online behavioural tracking,* (October 2012) available at http://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/privacy-considerations-of-online-behavioural-tracking, 7.

[13] S. Schoen, *New cookies technologies: Harder to see and remove, widely used to track you* (2009) available at https://www.eff.org/deeplinks/2009/09/new-cookie-technologies-harder-see-and-remove-wide.

[14] Clause Castellucia, *Behavioral tracking on the Internet, a technical perspective*, in *European Data Protection: In Good Health?* (Springer Netherlands, 2012), 29.

[15] Soltani, Ashkan, et al., *Flash Cookies and Privacy* (AAAI Spring Symposium: Intelligent Information Privacy Management, 2010).

[16] Niklas Schmücker *Web Tracking* (Department of Telecommunication Systems, SNET2 Seminar, Paper-Summer, 2011).

[17] Samy Kamkar, Evercookie – never forget (October 2011), available at: http://samy.pl/evercookie.

[18] Claude Castellucia, *Behavioral tracking on the Internet, a technical perspective*, in R.Leenes, *European Data Protection in good health?*, 25.

and so on. Although a consent is asked to start this function, the users generally do not measure the impact of their consent and the frequency and accuracy of the localization performed.

Finally, users lose their location privacy, defined as "*the ability of an individual to move in public space with the expectation that under normal circumstances their location will not be systematically and secretly recorded for later use*".[19] Location privacy is considered as part of each individual's privacy and is important to preserve. The concern here is that the new technologies enabling location tracking are becoming an increasingly widespread, cheap, easy, and accepted method to track users and collect valuable information.

2.1.2.6 Online Social Network Tracking

Social networks do not represent a particular "technology" or "tracking method" as the types of tracking techniques outlined above. Yet, online social networks constitute today an extremely popular trend encouraging people to stay continually "in contact", "be watched" or "followed". Surprisingly enough, such networks sometimes even promote the "tracking" as an asset of their website (for example, through an additional subscription fee, it could be possible for members to learn who other member looked at their personal details – like a cv – or who clicked on their profile to learn more about them).

Many users not only find this type of "tracking" trend normal but, all the more, they are seeking for it and are ready to pay extra to get it. On the other hand, there are social network members who usually consider the extra "tracking" features of social networking as "a necessary bad" that has to be tolerated, given that the privacy threats it entails are outweighed by the pleasure and other benefits resulting from users' interaction on social networking sites.

This type of tracking uses users' addiction to social networks in order to track every detail of the users' every-day activities including those of their close family and friends. A number of heavily-used and well-known networks, such as Facebook,[20] Twitter,[21] Pinterest[22] and LinkedIn[23] have recourse to this on-line tracking technique.

Take the example provided by A. Roosendaal: *the Facebook Like Button.*[24] According to Facebook, this widget allows users to share their interests and

[19] A. Blumberg, and P. Eckersley, *On locational privacy, and how to avoid losing it forever*, available at http://www.eff.org/wp/locational-privacy, 1.

[20] http://facebook.com/.

[21] http://twitter.com/.

[22] http://www.pinterest.com/.

[23] http://www.linkedin.com/.

[24] A. Roosendaal, *We Are All connected to Facebook . . . by Facebook!* in *European Data Protection: In Good Health?* (Springer Netherlands, 2012).

preferences between them. However, the scope of this tool is far broader then what Facebook seems to tell. As explained by Roosendaal, when the users click on the Like button, a login field opens and require the user to log in his Facebook account. After the user has logged in, a link will be created in the feed of news in Facebook and the network of the user will be able to see the content of the link. No need to be connected to an account to be tracked. The simple fact of visiting a website on which a Like button has been placed is sufficient to track Facebook members, and even non-members. Non-members can also be traced if they have already visited the social network website once. The scope is therefore enlarged to other subjects that the subscribers, and to other websites than the social media website. In addition, the awareness around this tracking technique is not very extensive and, therefore, the volume of data processed is incredibly high, which represent a very high financial value.

2.1.3 Risks of On-line Tracking

A major, common trend of some of the on-line tracking techniques discussed above is that the captured information is used for an array of intentions and purposes, predominantly for marketing reasons. It is rare that users are sufficiently aware of all the current, envisaged and potential (over time) uses of their data by the companies they are interacting with on the Internet. Yet, in our view, it is encouraging that some improvement can be noticed in this direction since the entry into force of the e-Privacy directive (as discussed below). Commercial and marketing agents have well understood the financial potential[25] of this knowledge and have built entire businesses on the potential of on-line behavioral tracking. Through the capturing and processing of different traces an internet user leaves on-line while visiting the same or different websites, companies are capable of creating user profiles.

Profiling is the recording and classification of behaviors. Although profiling has already been an intelligent marketing method based on information that can also be collected off-line (property and bank records, subscriptions selling, publicly available records, and so on), the Internet dynamics added an efficient, new dimension to it. Companies and on-line vendors can now track individuals *constantly*, and quite often, through a "voluntary" submission of personal information by the user to the network. Worse than that, many users consider the sharing of certain personal information through the internet as a "necessary bad" or a "societal necessity" (e.g., in order to adhere to a popular social network or to receive considerably

[25] *"In 2011, Europe's online advertising market grew 14.5 % year-on-year to a market value of €20.9bn in 2011. By comparison the overall European advertising market - excluding online - grew at just 0.8 % in the same time period":* See IAB, ADEX 2011, *Online Advertising in Europe (6th edition): Key Findings*, available online at http://www.iabeurope.eu/files/6613/6852/1900/2012_interact_presentation_final_delivered.pdf.

discounted offers by online vendors). Profiling in general has sparked an entire industry euphemistically labeled “Customer Relations Management” (CRM) or “Personalization”.[26] On-line profiling, in particular, has significantly expanded the sources for performing data correlations with a view to compiling users’ dossier of behavior, that may be correct but might even not. These dossiers of behavior may be used by marketers for target advertising but they can also be sold to governments for law enforcement or other government related purposes (national security, national defense and so on).

Moreover, today’s behavioral tracking techniques are so powerful that they allow to link anonymous data to specific individuals. The Like Button of Facebook is a good example. Marketing companies’ websites being in possession of named (true or not) profiles which are not properly secured, are more vulnerable to cyber incidents and data breach threats. It is probably not exaggerating to say that all these profiles could at the end be accessed by professional hackers, either to commit criminal acts against the profiled individuals or in their name by using their profile and identity.[27]

Further, one of the ultimate objectives of the on-line behavioral tracking is the personalization of the website content presented to the users. Despite the well-intended purpose of method (gain in time, result-oriented web surfing, tailored content to the users’ needs), it is not always a given that the operator using automated web personalization through cookies knows better the user’s preferences and needs than the user himself. On the contrary, a user could arguably claim that, as he is automatically directed to content which is presumed to be of interest to him, he may misses the opportunity to look at other content which is useful to him or which becomes relevant because of a change in the person’s habits or way of living. At the end, the tracking technology restrict users’ freedom to look at “neutral” information being objectively communicated to all users.

2.2 On-line Tracking Under the Current Data Protection Legal Framework

On-line tracking as a market trend supported by specific technologies (as discussed above) falls under the applicability scope of the core data protection regulation currently in-force in Europe. We briefly outline below how the major rules and core foundations of the applicable data protection framework become relevant to on-line tracking. This means that, today, on-line tracking technologies are not developed and used in a legal vacuum as explained below.

[26] Electronic Privacy Information Center, *Privacy and Consumer Profiling, “The Product is you”,* available at http://www.epic.org/privacy/profiling.

[27] Along these lines, note the “@N” incident on Twitter: http://arstechnica.com/security/2014/02/twitter-restores-50000-n-username-to-its-owner/.

2.2.1 Personal Data Protection Directive

The processing of personal data by the use of on-line behavioral techniques as the ones referred above is subject to the requirements of the general EU Data Protection Directive (Directive 95/46/EC, herein the "Data Protection Directive"). The cornerstone principles of this directive must be observed and applied effectively by the parties involved in on-line tracking. Besides the citizen being the party who can benefit from the protection of this law, other parties concerned are: i) vendors of such on-line tracking technologies (software/hardware companies) and ii) the implementers of such applications (advertising and market research companies, as well as any other company wishing to reap up the benefits of such technologies for their own marketing and selling activities or other purposes).[28]

On top of the Data Protection Directive, another EU legal act specifies the requirements of the processing of personal *data in the electronic communications sector (EU Directive 2002/58 as amended).* One of the major changes brought by the latter Directive, the so-called e-Privacy Directive, tackled a core aspect of the subject matter under discussion here, namely the type of consent that should be obtained from the individual subject to on-line tracing techniques, including on-line behavioral tracking.

Specifically, current Article 5 §3 of the e-Privacy Directive reads:

> *Member States shall ensure that the storing of information, or the gaining of access to information already stored, in the terminal equipment of a subscriber or user is only allowed* **on condition that the subscriber or user concerned has given his or her consent**, *having been provided with clear and comprehensive information, in accordance with Directive 95/46/EC, inter alia, about the purposes of the processing. This shall not prevent any technical storage or access for the sole purpose of carrying out the transmission of a communication over an electronic communications network, or as strictly necessary in order for the provider of an information society service explicitly requested by the subscriber or user to provide the service.*

In the same vein, Recital 66 of the directive which introduced the latest amendments to the e-Privacy Directive,[29] stressed the importance for users to be provided with clear and comprehensive information when engaging in an activity which could result in behavioral tracking. In the same Recital, it is emphasized that the methods of providing information and offering the right to refuse should be as user-friendly as possible.

Although the aspect of user notice (consent) has appeared to be probably the biggest challenge in the interpretation of the revised e-Privacy directive (see below, Sect. 2.2.2.4), the other privacy foundations as enshrined into the Data Protection Directive are also worthy of commenting.

[28] To note that the "on-line" tracking market is quite sophisticated and other market actors besides the categories cited here (vendors of on-line tracking tools and the companies involved in on-line tracking) may also be subject to data protection rules.

[29] *Supra*, footnote 8.

2.2.2 *Applicability of the Core Foundations of Personal Data Protection*

2.2.2.1 Purpose Limitation

Personal data must be collected for a purpose defined in advance.[30] With regard to on-line tracking tools, the purpose for collecting data must be legitimate. The collection and storage of data must then be aligned with the defined purpose.[31] In addition, the collection of data cannot override the purpose for which the on-line user has given his consent.[32] Let us take as example the privacy statement published on the website of a market research organization explaining that, while it uses on-line tracking tools, the captured data will only be used to build up statistics on the number of visits that "hit" the website. If the market research company then uses the data for another purpose that is not directly linked to verifying the initial purpose, for example in order to sell those data to a number of companies interested in sending their on-line surveys to new prospects, then the "purpose limitation" rule has clearly been infringed.

2.2.2.2 Data Subject Notice

This requirement sets forth the obligation of the data controller to provide clear information to the internet users about the collection and processing of their personal data.[33] The requirement is directly relevant to on-line monitoring activities, especially because a great part of the data processing operations is "invisible" to the individual. Moreover, on-line monitoring often involves many actors, meaning the company interacting with the individual but, very often, the "processor" who will analyze and correlate the data by using marketing intelligence or other techniques and probably other data "recipients". It is a general but correct perception that on-line activities increase by definition the risk that the data will be spread around with no ultimate control from the end-user.

2.2.2.3 Proportionality

Personal data must be adequate, relevant, and not excessive in relation to the purposes for which they are collected and/ or further processed. Let us take again

[30] Article 6 of Directive 95/46/EC.

[31] Article 6(1)(b) of Directive 95/46/EC.

[32] Article 29 Data Protection Working Party, Opinion 2/2010 on online behavioural advertising, adopted on 22 June 2010, 00909/10/EN WP 171, p. 20.

[33] Article 10 of Directive 95/46/EC.

the example of the market research organization referred to above. In the company's privacy statement there is no word about whether the company is using personally identifiable information or other forms of data (aggregate, de-identified, etc.) to achieve the purpose of data collection. However, in the light of the purpose formally mentioned in the privacy statement (checking the number of visits on the website), one can easily understand that the company in question does not need to process personal data. On the contrary, to attain the declared purpose, the market research company is even obliged to use on-line monitoring means and techniques which will enable it to track users anonymously, thus without having to know exactly the person (or an identifier of him) being behind each "click" on the company's website. There are many on-line tracking applications which are designed, or could be reconfigured, in order to collect data only on an aggregate level. Such method of using aggregate information instead of personal identifiers or other personal data could be used in our example here to align with the proportionality principle.

2.2.2.4 Obligation to Obtain Prior Consent

The consent rule practically means that the implementers of the on-line tracking tools must seek to obtain the prior acceptance of the on-line user before any tracking begins.[34]

There are many ways to collect consent, and to, *a priori,* meet the requirements of article 5(3) of the Directive. Nevertheless, the practice and doctrine have demonstrated that the concept of consent as stated in the Directive is not very clear and requires further developments.[35]

Pursuant to article 5(3), the consent should be obtained after having informed the data subject on the nature and purpose of the collection. Adapted to the use of tracking tools, this means that the subject should be informed prior to the placement of tools intended to collect information on individuals navigating in the World Wide Web.

In practice, many techniques have emerged to meet the requirements of consent. Yet, not all of them are necessarily in line with the legal prerequisite of consent as laid down in the e-Privacy Directive. In its opinion on on-line behavioral advertising, the Article 29 Working Party provides an interpretation of the notion of "consent" as meant in the latter Directive. In the same opinion, the Article 29 Working Party attempts to lay the foundations of a correct interpretation of the obligation to obtain prior and informed consent.[36]

[34] Article 5(3) of Directive 2002/58/EC.

[35] Matthew S. Kirsch, *Do-Not-Track: Revising the EU's Data Protection Framework to Require Meaningful Consent for Behavioral Advertising*, (XVIII RICH. J.L. TECH. 2) available at http://jolt.richmond.edu/v18i1/article2.pdf, 12-18.

[36] Article 29 Data Protection Working Party, Opinion 2/2010 on online behavioural advertising, adopted on 22 June 2010, 00909/10/EN WP 171, 12-17.

Consent Obtained by Browser Settings

According to the Article 29 Working Party, a consent obtained by means of browser settings is not sufficient under the law. Obtaining the consent by way of the browser settings relies on the placing of cookies as default. If the user does not turn the cookie function off, the default configuration remains intact, implying that the user has consented to the cookie given that he has not actively prompted to change the browser settings (although he was given the information to do so). Such "consent" obtained "by default" has been questioned by the European regulator.

Consent Given by Opt-out Mechanisms

Service providers are increasingly using opt-out mechanisms enabling users to refuse receiving target advertising. Although we can recognize the benefits of this approach, the mechanism is not adequate and sufficient as a way to obtain informed consent.[37] First, the lack of users' awareness of users is tricky, as many of them do not know where to opt-out despite the fact that they may be given the possibility to do so. Second, when the user does not opt-out, the provider will consider this as an implicit consent. However, the consent should be derived from an affirmative action of the user, and not from inaction.

Prior Opt-in Consent

The Article 29 Working Party has interpreted the article 5(3) in a strict way: the user should first be provided with information on the processing in general and, second, consent to the processing and collection of data. These two conditions are cumulative. It must be given prior to the processing.[38] Furthermore, the consent should be the result of an affirmative action of the users. In addition, the consent should be considered as valid only for a limited period of time. Finally, the on-line users should be given the possibility to revoke their consent easily.

2.2.2.5 Data Destruction/Retention

This requirement basically means that any personal data that have been collected and used throughout the on-line tracking operations must at the end be destroyed,

[37] Article 29 Data Protection Working Party, Opinion 2/2010 on online behavioural advertising, adopted on 22 June 2010, 00909/10/EN WP 171, p. 15.

[38] E. Kosta, *Peeking into the cookie jar: the European Approach towards the regulation of cookies,* (International Journal of Law and Information Technology, vol. 21, No 4, 2013), 392.

at least when they are no longer needed for achieving the purpose of data collection or at a shorter time period (that has to be defined by the company using the tracking technique).

Data retention associated with on-line tracking methods is even more challenging than other more ordinary forms of data processing. Let us imagine the market research company of our example above, attempting to meet practically the data destruction/retention requirement while the purpose of data collection is now user profiling. Having this new purpose in mind, the company has deployed a tracking technique online (based on certain observer tags or cookies for example). In this case, these data are precisely collected now with the intention to be used for long time-periods. Especially in cases where those data will form the data repository (or "stock") against which new data from "new" users, will continue to enter and will require correlation. Thus, the more data the company has, the more chances it has to mix correctly all these data and form more "accurate" profiles It is quite common that companies like this of the example will use aggregate or anonymous data especially if the storage entails data retention for a long period of time. Yet, in case that, the company of the example, probably assisted by specialist service providers achieves to correlate the data at a later point of time with individual users, namely to re-identify individuals, there is very little likelihood and only when specific conditions are fulfilled,[39] that such correlation activity will be compliant with data protection rules. Second, even if the company finds out satisfactory ways to achieve its purpose while meeting the data destruction requirement (which is technically possible), another challenge it may have to encounter is how controlling that the range of service providers it cooperates with in order to implement the profiling technique, to map data and adduce conclusions of such mapping. The situation becomes more complex if the market research organization in question may request services from a cloud provider which will, for example, provide data repository services or will help in data analysis and users' clustering in specific profiles.

At the end, the market research company will have to ensure that appropriate data deletion and retention practices have been implemented not only by itself but also from the range of providers mentioned above.

2.3 Future Personal Data Protection Framework: How Will It Affect Behavioral On-line Tracking?

In order to address efficiently the challenge of personal data protection in view of the economic, market, and technological challenges since the adoption of the Data Protection Directive (1995), a reform of the regulatory framework is now underway.

[39] Such as clear and specific notice to user and consent.

Accordingly, a proposal for a new Data Protection Regulation likely to replace the Data Protection Directive is now under negotiation for adoption by the European Parliament and the Council.[40]

The basic motives of the EU regulators' decision to reshape the current data protection regulation are directly relevant to the topic of this article: according to Recital 5 of the new act under discussion, "*...the scale of data sharing and collecting has increased spectacularly. Technology allows both private companies and public authorities to make use of personal data on an unprecedented scale in order to pursue their activities. Individuals increasingly make personal information available publicly and globally*".

Although the adoption of the new draft is not certain yet and despite the fact that the content of the draft under discussion here will in all likelihood still change, it is widely admitted that a regulatory reform in the area of personal data protection is necessary and must continue. Based on this assumption, we summarize below a few elements of the proposed Data Protection Regulation (herein "Regulation") which, in our view, if they are adopted, they will have a significant impact on the way on-line tracking technologies and all the market actors behind it (designers, vendors, and implementers) will have to deploy such technologies in the future.

The points of attention listed below are not exhaustive although, in our opinion, they depict noticeable changes if they come through:

2.3.1 Scope of Application

It often happens that companies not established in Europe are those conducting on-line tracking. Under the current application scope of the Data Protection Directive, such companies are highly likely to escape the rigorous European privacy rules, especially if it is difficult to demonstrate that the means used to process the personal data are established in Europe. To change this, the Regulation suggests that non-based EU companies (be controllers or processors) will henceforth be subject to the controls and requirements set forth in the new legislative framework insofar as they perform activities related to "*the monitoring of data subjects*".[41] It is the first time that primary regulation in Europe renders the monitoring (including the on-line one) as a sufficient element *per se* to decide on the applicability of the European privacy laws. In addition, the Regulation sheds some more light into the activities that one may take into account to determine whether a company performs *monitoring*.

[40] Proposal for a regulation of the European Parliament and of the Council on the protection of individual with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), COM(2012)0011 – C7 0025/2012 -2012/0011 (COD). To be noted: this version of the draft act may not be the most recent one at the time this article will be published.

[41] *Supra* reference 41, art. 3 *"Territorial Scope",* §2, (b).

Therefore, any technique consisting of applying a “profile”, particularly in order to take decisions concerning a person or for analyzing or predicting such person’s personal preferences, behavior or attitude fall under the scope of “monitoring”.[42]

In our view, this is a considerable change clearly demonstrating that on-line tracking was one of the key factors taken into account to decide on the need of legislative reshuffling.

2.3.2 Definitions

Another element reaffirming the intention of the regulator to confirm that the privacy rules will be relevant to any type of monitoring and profiling affecting individual’s privacy is the new definition of “profiling” currently inserted in the new text. Accordingly, profiling is defined as “*any form of automated processing of personal data intended to evaluate certain personal aspects relating to a natural person or to analyse or predict in particular that natural person’s performance at work, economic situation, location, health, personal preferences, reliability, or behaviour”*.[43]

We infer from the new text, that data mining and data correlating methods enabling the evaluation, analysis, or forecasting of any parameter of the economic, social, and working life of an individual; as well as of any aspect of his personality (interests, preferences, etc.) may be caught by this definition of “profiling”. More precisely on on-line tracking tools, the Regulation explicitly mentions that “cookie identifiers” (as well as RFID tags) should be considered as personal data eligible for protection under the EU privacy regulatory framework on condition that such identifiers relate to identified or identifiable natural person.[44]

2.3.3 Consent

The requirements around the consent, representing probably the most critical factor of legitimizing on-line tracking and profiling techniques, become stricter under the Regulation. Although the main conditions for recognizing that the consent provided is valid do not change in essence (freely-given, specific, and informed), the proposed text sets forth explicitly that mere use of a service or inactivity should not constitute a valid consent.[45] On this point, the Regulation seems to be consistent with the conditions set forth on the e-Privacy Directive and the market practice that is now being shaped around the implementation of such cookies’ consent, requesting an

[42] *Supra* reference 41, Recital 21.

[43] *Supra* reference 41, art. 4 *“Definitions”,* §3a.

[44] *Supra* ref. 41, Recital 24.

[45] *Supra* ref. 41, Recital 25.

affirmative action of the on-line user (be it through clicking on an "I accept" or "ok" box on a website banner or by use of another technique) before installing the tracking application. In consequence, pre-configuration of the browser settings so that cookies are installed unless the individual opts out do not appear to be in-line with the "affirmative" action that the notion of "consent" as confirmed by the Regulation seems to request.[46]

If the current language of the Regulations' text over the user's consent is adopted the notion of consent through an action (as set forth in the e-Privacy directive) will be reinforced.[47] Consequently, companies deploying on-line tools on their websites will increasingly be obliged to promote solutions explicitly supporting an "action" from the individual who agrees to be subject to tracking. If this element is considered as a confirmation of prerequisites already set forth in current laws (e-Privacy directive), an innovative element of the Regulation concerns the burden of proving that a valid consent has been provided. According to the Regulation's text under adoption, in case that the individual subject to tracking questions the mechanism through which he provided his consent, it will be the controller who will have the obligation to demonstrate that the said individual has indeed provided his consent.[48]

Another innovative element is that, for the first time, an EU primary law on privacy will emphasize explicitly the conditions that should be fulfilled to accept that the consent given by a child is valid. This is particularly relevant when we talk about internet usage, knowing how manychildren are using the internet today and, hence, how vulnerable they could be to on-line tracking techniques. Under the Regulation, it seems that children above 13 are considered mature enough to provide valid consent, whereas, the consent of the parent or guardian is requested for children under 13.[49] Although one could argue about the practical effect of such provision (which might mean practically that a clear "opt in" by parents is requested for children to be able to continue navigation on a website), it is already a positive sign that the new rules recognize that children merit more special attention than adults when they have to make a choice affecting their privacy.

[46] The fact that browser settings are not yet sophisticated enough to secure by themselves a user's affirmative action has been stressed in many recommendations of Member States' privacy oversight bodies, such as the Information Commissioner's Office in the UK (ICO). In a recent guideline provided on the use of cookies of ICO, it is mentioned that "*For consent to be clearly signified by the browser settings it would need to be clear that subscribers had been prompted to consider their current browser settings and, had either indicated in some way they were happy with the default, or have made the decision to change the settings*", Information Commissioner's Office, *Guidance on the rules on use of cookies and similar technologies* (May 2012, v. 3, p. 15). In the same vein, the Regulation states that "*the use of default options which the data subject is required to modify to object to the processing, such as pre-ticked boxes* (or, we infer, browser settings – our addition -) *does not express free consent* (Supra ref. 41, Recital 33).

[47] It is noteworthy that the Regulation seems to introduce a new right of the data subject, being the right *to object to profiling* (Supra ref. 41, art. 10a *"General principles for data subject rights"*, §2.

[48] *Supra* ref. 41, Recital 7 *"Conditions for Consent"*, §1.

[49] *Supra* ref. 41, Recital 29.

2.3.4 Notice

In the same vein as the requirements around consent, the Regulation seems to strengthen the conditions regarding the information data controllers must provide to the data subjects about the processing of their personal information.

First, the Regulation explicitly requests data controllers to communicate appropriate *policies* informing the data subjects about how their personal information is handled. This requirement means primarily that data controllers shall draft in a clear and user-friendly language relevant personal data protection policies.[50] For internet users, it is particularly interesting that the new text requires now explicitly that such policies are easily accessible (for example, through an obvious, catchy to the eyes, reference on the company's website) and drafted in clear and plain language. What is more noteworthy is that the Regulation makes an explicit reference to on-line advertising requesting companies involved in such practices to clearly indicate to the on-line users if personal data are collected, by whom and for what purposes.[51] In particular, websites addressed to children must communicate in a language that children can understand the above elements.

Second, in order to ensure that the minimum requirements of a data protection policy are covered in the documentation that all controllers will be providing to data subjects and this in a consistent and concise language, the Regulation suggests the adoption of a series of particulars.[52] It will be quite interesting to follow how the mandatory content of policies as meant by the EU regulator (i.e., the adoption of the specific particulars set forth now in the Regulation) will consistently be followed by the market practice. This will probably be even more challenging for non-EU based companies, such as the ones active in on-line tracking and profiling that as noted above, will become subject to the requirements of this Regulation. Such foreign companies will in all probability not have similar "notice standards" (particulars) in the country where they are based.

Third, it is particularly relevant to the context discussed herein, that the EU regulator envisages extending the scope of information that should be communicated to the data subjects to include, *"where applicable, information about the existence of profiling, of measures based on profiling, and the envisaged effects of profiling*

[50] Yet, in our interpretation, the Regulation covers indirectly the adoption of other internal regulations and policies, except from the data protection policies, if these would be relevant to the protection of personal information too (e.g., documentation relevant to the security of information, data classification, confidential information and so on).

[51] *Supra* ref. 41, Recital 46 reads: "*. . . This* (the principle of transparency – our addition) *is particularly relevant where in situations, such as online advertising, the proliferation of actors and the technological complexity of practice makes it difficult for the data subject to know and understand if personal data relating to them are being collected, y whom and for what purposes*".

[52] It appears that the current draft of the Regulation requests the adoption of specific graphical forms showing whether personal data are collected, stored, shared with other parties and so on, that would be made easily visible and clearly legible on a website. Supra ref. 41, article 13a and Annex 1.

on the data subjects; ... ".[53] This is a real novelty introduced by the Regulation. If this phrasing is finally maintained in the adopted text, this requirement may considerably change the content and level of detail in the majority of the privacy notices and statements that companies currently publish on their websites to inform their customers of on-line profiling, tracking, and behavioral monitoring activities. In most of the cases today, it is a common (and we would even say, widely acknowledged practice) to apply very general and all-inclusive language in order to describe on-line tracking activities. Thus, standard *language* is often used by service providers, such as that cookies are used "*to enhance the user's experience on the website*" or "*for marketing purposes*" or to "*improve the quality of the (provider's) website*", and so on. Such type of wording may not be sufficient anymore when the new law comes into force.

Finally, relevant to the notice requirement is the new right formulated in the Regulation with regard to end-user's objection to profiling. Accordingly, the user shall be informed about the right to object to profiling in a *highly visible manner.*[54]

2.3.5 The Right of Erasure ("Right to Be Forgotten")

Besides the rule of data destruction (outlined above, Sect. 2.2.2.5), the Regulation introduces a new right of the data subject/user, being the right to demand from the data controller that he deleted the user's personal data or, more relevant to the on-line activities, *that the data controller stops copying or replicating* such data.[55] Relevant to the example of the market research company referred to above (Sect. 2.2.2.5), according to the new text, the data controller shall also take *all reasonable steps* to ensure that third parties having received the user's data will erase them accordingly. Moreover, if possible, the data controller will have the obligation to inform the on-line user of the action third parties have taken to align with this requirement.[56] Yet, the Regulation provides a number of derogations to the obligation to erase the personal data, which may actually be used in the case of on-line profiling/monitoring too. Indicatively here, if the controller needs to keep the personal data for evidence purposes or if the storage application used does not technically allow data erasure, it will be possible to archive those data and not satisfy the user's request of erasure. The requirements that should be fulfilled for the archiving of the collected personal data in this case are spelled out in the Regulation.[57]

Some discussion of the problems that might arise here is advised.

[53] Supra ref. 41, art. 14, new letter (ga).

[54] Supra ref. 41, art. 20, §1.

[55] *Supra* ref. 41, art. 17, §1.

[56] *Supra* ref. 41, art. 17, §2.

[57] *Supra* ref. 41, art. 17, §4.

2.3.6 Data Protection "by Design"

The new concept of data protection "by design" as introduced in the Regulation will oblige both data controllers and processors to ensure that they will implement appropriate technical and organizational measures and procedures to protect the personal information. The time for choosing the appropriate measures and procedures should be the time at which the purposes and the means of the data processing operation are determined, as well as the time at which the said processing starts.

The privacy by design principle is one of the most innovative elements of the Regulation: *"this approach transforms consumer privacy issues from a pure policy or compliance issue into a business imperative"*.[58] According to this requirement, privacy concerns should be incorporated in the design phase of new information technologies, business practices, and networked infrastructures. As the famous quote "better preventing than curing", business should focus on privacy during the entire lifecycle of the management of personal data and should implement safeguards in order to protect those data.

In the context of on-line tracking techniques, the concept of "data protection" by design is particularly pertinent. Threats and risks that a specific "intelligent" on-line application may entail to the user's privacy shall be determined from the design phase of the tool once the purposes of the envisaged data tracking and the technical options to achieve those are formed. At the end, the "data protection" by design will not only affect tracking technology implementers (i.e., companies implementing the tool and other parties supporting it in the implementation or the data analysis, etc.) but also the designers (and probably vendors) of such tools. This is because, in order to satisfy the requirement put upon them, the data controller and/or processor will have to ensure that: a) the design of the on-line tracking tool can be technically adjusted to fit the data processing purpose and the controls that will be put in place and b) "privacy protection" requirements have been considered right from the phase of product conception in order to avoid costly adjustments and changes at the implementation phase.

2.3.7 Towards a "Privacy Friendlier" Internet Tracking: The Role of Society, (Social) Media and Education

The provisions of the New Regulation outlined above constitute only a limited part of many provisions that will potentially have an impact on the deployment of online tracking technologies and the way the designers and users of such technologies

[58] Cavoukian A., *Privacy by Design in Law, Policy and Practice, A White Paper for Regulators, Decision-makers and Policy-makers,* (August 2011, Information and Privacy Commissioner, Ontario, Canada) available at http://www.ipc.on.ca/images/Resources/PbDBook-From-Rhetoric-to-Reality.pdf, 13.

will process personal data captured through them. Some more examples of legal measures that will affect companies' conducting profiling/on-line activities are for example: the definition of high fines' scales to sanction data protection infringements or the obligation to conduct privacy impact assessments before the implementation of a technology or project which may be threatening to individuals' privacy or the mandatory designation of personal data protection officers in data processing environments. At the time of drafting this article, the relevant articles of the Regulation are being reviewed meticulously and their exact scope may change.

Should however regulation be perceived as a "panacea" to the exponential growth of on-line tracking trends in our society? Definitely, no. The letter of laws is never a solution *per se* if such laws are not accompanied by measures that can effectively raise awareness about the problems explaining their adoption and on how the rules should be interpreted in practice. Let us also not forget that for a legal measure to be effective, it is necessary that the societal actors concerned accept at the end the "*raison d'être*" of the act and implement the rules effectively.

Translating the above experience in the case of "on-line" tracking, means that besides the regulators' intention to provide enhanced data protection through a stringent legal framework, there is a lot more that needs to be done to objectively educate users about the opportunities and risks entailed while surfing on the internet. If social networking is a "privacy-evasive" trend of today's society, it can also be transformed into a very powerful tool to promote privacy and educate users. Along the same lines, self-regulatory approaches, and other initiatives encouraging the private-public dialogue, as well as standardization work could help market stakeholders and public interest bodies to take actively part in the way the new or amended data protection framework should be interpreted. European institutions and agencies, but also public-private initiatives at country level, could be the instigators of such dialogue that would require academy and data protection oversight bodies to engage in it actively.

If regulatory reforms are difficult to be launched and their concrete effects become many times visible only in the long term, soft regulation and societal initiatives may prove to be more efficient on condition that they are coordinated well and motivate market stakeholders to participate.

2.4 Conclusion

The current European legislation, namely the Data Protection Directive and the e-Privacy Directive (after its last revision) constitute the basic legal framework for the protection of the privacy of on-line users when they become subject to on-line tracking techniques. If the new Regulation on personal data protection is finally adopted without major changes to the latest draft published, the manufacturing and design industry of behavioral tracking tools, as well as the companies that implement on-line tracking technologies, will be encountered with stricter requirements in terms of personal data protection. To summarize, these requirements mainly refer to the adoption of documentation, procedures, and controls that companies active in the design phase or using on-line tracking applications will have to create or update. The Regulation seems to recognize explicitly that data collection and processing through tracking techniques pose major threats to citizen's privacy. Therefore, it sets forth new rights of the data subject particularly relevant to on-line activities (right to data erasure, right to object). Finally, the Regulation's text in the current version attempts to switch the "mindset" of designers, controllers and processors to better "predict" privacy than "remedy" privacy, by introducing the core principle of data protection "by design".

It is however the view of the authors that, in practical terms the new (and probably, more rigorous) legal imperatives will not bring the desired change if the perception of the individuals around the fancy "on-line" tools they are offered today to facilitate their integration in the modern society does not change. Additional and stricter regulatory conditions will not be sufficient without sensitizing business about the importance of implementing controls and procedures towards their software vendors and the need for strengthening the privacy contractual guarantees in the services agreements they have with them. Moreover, this also means that some extra effort should be taken to educate on-line users, especially those of young age, of what they should avoid and dare refuse on the internet.

Other initiatives stemming from the public interest stakeholders, as well as professional organizations, could serve as an efficient remedy to today's exponential and abusive on-line tracking of citizens. Dedicated self-regulation on this subject matter, awareness campaigns for citizens to introduce self-defense tools (a number of those are available on the market today[59]), more education about citizens' rights and the recourse mechanisms available in case of infringements could be some other supplementary ways, next to the law, to render citizens' right to control their data meaningful and enforceable in practice.

Bibliography

Academic Sources

Blumberg A. and Eckersley P. *On locational privacy, and how to avoid losing it forever*. Available at http://www.eff.org/wp/locational-privacy.

Cavoukian A. *Privacy by Design in Law, Policy and Practice, A White Paper for Regulators, Decision-makers and Policy-makers*. August 2011. Information and Privacy Commissioner, Ontario, Canada. Available at http://www.ipc.on.ca/images/Resources/PbDBook-From-Rhetoric-to-Reality.pdf.

Castellucia C. *Behavioral tracking on the Internet, a technical perspective*. In *European Data Protection: In Good Health?* Springer Netherlands, 2012.

Eckersley P. *What does the "Track" in Do Not Track Mean?* 19 February 2011. Electronic Frontier Foundation. Available at https://www.eff.org/deeplinks/2011/02/what-does-track-do-not-track-mean.

[59] ENISA, *Privacy considerations of online behavioural tracking*, October 2012, available at http://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/privacy-considerations-of-online-behavioural-tracking, 18.

Eckersley P. *How unique is your web browser?* 2010. Privacy Enhancing Technologies, Springer Berlin Heidelberg. In *Consumer Privacy Law 2: Data Collection, Profiling and Targeting*. July 16, 2009. Law And The Internet. L. Edwards & C. Waelde, eds., Hart Publishing. Available at https://panopticlick.eff.org/browser-uniqueness.pdf.

Goldberg I., Wagner D., Brewer E. *Privacy-enhancing Technologies for the Internet.* 1997. Proceedings of IEEE COMPCON '97. Available at http://www.cs.berkeley.edu/~daw/papers/privacy-compcon97.ps.

Hildebrandt M. *Profiling: from data to knowledge*. 2006. DuD: Datenschutz und Datensicherheit 30.

Kirsch Matthew S. *Do-Not-Track: Revising the EU's Data Protection Framework to Require Meaningful Consent for Behavioral Advertising.* XVIII RICH. J.L. TECH. 2. Available at http://jolt.richmond.edu/v18i1/article2.pdf.

Kamkar S. *Evercookie – never forget*. October 2011. Available at: http://samy.pl/evercookie.

Kosta E. *Peeking into the cookie jar: the European Approach towards the regulation of cookies.* 2013. International Journal of Law and Information Technology, vol. 21, No 4.

Roosendaal A. *We Are All connected to Facebook... by Facebook!* in Gutwirth S., Leenes R., de Hert P., Poullet Y. (Eds.). *European Data Protection: In Good Health?* 2012. Springer Netherlands.

Schmücker N. *Web Tracking*. 2011. Department of Telecommunication Systems, SNET2 Seminar, Paper-Summer.

Schoen S. *New cookies technologies: Harder to see and remove, widely used to track you*. 2009. Available at https://www.eff.org/deeplinks/2009/09/new-cookie-technologies-harder-see-and-remove-wide.

Soltani A. et al. *Cookies and Privacy*. 2010. AAAI Spring Symposium: Intelligent Information Privacy Management.

Swaminatha T. M. *Privacy Enhancing Technology*. Privacy Enhancing Technology. Guidelines and Testing Methodology, W3C/QA Position Paper. Available at http://www.w3.org/2001/01/qa-ws/pp/tara-swaminatha-cigital.html.

Business Sources

Article 29 Data Protection Working Party, Opinion 2/2010 on online behavioural advertising, adopted on 22 June 2010, 00909/10/EN WP 171.

Electronic Privacy Information Center. *Privacy and Consumer Profiling, "The Product is you".* Available at http://www.epic.org/privacy/profiling.

ENISA, *Privacy considerations of online behavioural tracking*, (October 2012) available at http://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/privacy-considerations-of-online-behavioural-tracking.

Geuss M. *Twitter restores $50,000 @N username to its owner. A simple social engineering attack list Naoki Hiroshima a very valuable handle.* 26 February 2014. Available at http://arstechnica.com/security/2014/02/twitter-restores-50000-n-username-to-its-owner/.

IAB, ADEX 2011, *Online Advertising in Europe (6thedition): Key Findings*, available at http://www.iabeurope.eu/files/6613/6852/1900/2012_interact_presentation_final_delivered.pdf.

Regulator Sources

Communication from the Commission to the European Parliament and the Council on promoting data protection by privacy-enhancing technologies. COM(2007)228 final. Available at http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52007DC0228&from=EN.

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. COM/2010/0609 final. Available at http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52010DC0609&from=EN.

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, (31.07.2002).

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 (Data Protection Directive). OJ L 281, (23.11.1995).

Draft report on the proposal for a regulation of the European Parliament and of the Council on the protection of individual with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). COM(2012)0011 – C7-0025/2012 – 2012/0011(COD). Available at http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/pr/922/922387/922387en.pdf.

Information Commissioner's Office. *Guidance on the rules on use of cookies and similar technologies.* May 2012. Available at http://ico.org.uk/~/media/documents/library/Privacy_and_electronic/Practical_application/cookies_guidance_v3.pdf.

Proposal for a regulation of the European Parliament and of the Council on the protection of individual with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), COM(2012)0011 – C7 0025/2012 -2012/0011 (COD). Available at http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf.

Study on the economic benefits of privacy-enhancing technologies (PETs), Final Report to The European Commission DG Justice, Freedom and Security, Prepared by London Economics, July 2010. Available at http://ec.europa.eu/justice/policies/privacy/docs/studies/final_report_pets_16_07_10_en.pdf.

Part II
Taming the Future: Assessments of Risks in the Sphere of Privacy and Data Protection

Chapter 3
A Systematic Approach to the Legal Evaluation of Security Measures in Public Transportation

Christian Ludwig Geminn and Alexander Roßnagel

Abstract This paper explores the need for a systematic approach when evaluating security measures in the context of public transportation. Subsequently, a method for the evaluation of security measures is presented. This method should be used by decision makers tasked with the acquisition and implementation of security measures. It promotes the use of fundamental rights and principles as a basis for the evaluation, as well as the benefits of going beyond minimum legal requirements.

Keywords Legal Evaluation • Security Measures • Method • Public Transportation

3.1 Introduction

In 2008, the global market for security products and services exceeded the mark of 100 billion Euros for the first time and has grown by about 5–7 % every year since.[1] The share of the European market in the global market is 30 %.[2] These numbers are indicators of the high expenses in this sector. An investment in a certain security measure is a long-term investment. No end user can afford misinvestments due to high acquisition and follow-up costs, especially in the field of public transportation which is traditionally one of the focal points of the security debate. It is thus very important for any decision maker to choose a security product that can be used without coming into conflict with the law. Furthermore, the security measure must be socially accepted; it must not deter potential passengers from travelling, thus threatening the business model of a public transportation operator.[3]

[1] This paper has been adapted and translated from Christian Ludwig Geminn, *Rechtsverträglicher Einsatz von Sicherheitsmaßnahmen im öffentlichen Verkehr* (Wiesbaden: Springer Vieweg, 2014).

[2] Printed matter (Drucksache) of the German Bundestag No. 17/8500, 6.

[3] In the context of this paper, public transportation encompasses civil aviation, bus and train.

C.L. Geminn (✉) • A. Roßnagel
Research Center for Information System Design (ITeG), Kassel University, Kassel, Germany
e-mail: c.geminn@uni-kassel.de; a.rossnagel@uni-kassel.de

S. Gutwirth et al. (eds.), *Reforming European Data Protection Law*,
Law, Governance and Technology Series 20, DOI 10.1007/978-94-017-9385-8_3

Finding such a product can be a challenging process due to the fact that the market for security products is international. Developers that operate internationally will often lack the competence or the willingness (for example for reasons of cost-efficiency) to take the provisions of several legal systems into account when developing new products, and to create products that can be used in a multitude of countries. Other developers may only create security measures or offer security services with a single country in mind that offers a large market for security related products and services. A decision maker who is tasked with the acquisition or the implementation of security measures is thus faced with the dilemma that in order to solve a security problem he or she can choose from a whole range of products. The technological advantages and disadvantages of these products are usually apparent, but they do not offer any guarantee that they can be used without violating existing laws in the legal system of the country in which the decision maker operates.

Parameters like those that can be found in Part A of the Annex to Commission Regulation (EC) No. 272/2009[4] in the form of a catalogue containing acceptable methods for the screening of passengers, luggage and freight in civil aviation do not offer much assistance when selecting a concrete product. Such parameters offer nothing more than a list of methods that are acceptable in principle, but they do not offer indications on how a method has to be shaped precisely, both in a technological and an organisational sense. Security measures that violate the law however cannot and must not be authorised and operated.

The following chapters will propose a solution by presenting a method for the legal evaluation of security measures. This method is a variant of a method for a legally compatible technology design which was introduced by *Roßnagel* and the Project Group Constitutionally Compatible Technology Design.[5] It has since then been used extensively in a number of contexts,[6] including the legally compatible design of security measures.[7]

[4] Commission Regulation (EC) No. 272/2009 of 2 April 2009 supplementing the common basic standards on civil aviation laid down in the Annex to Regulation (EC) No. 300/2008 of the European Parliament and of the Council, L 91/7.

[5] KORA (concretisation of legal requirements; German: Konkretisierung rechtlicher Anforderungen). The method was introduced in Volker Hammer, Ulrich Pordesch and Alexander Roßnagel, "KORA, Eine Methode zur Konkretisierung rechtlicher Anforderungen zu technischen Gestaltungsvorschlägen," *Infotech/I + G* 1 (1993): 21 and Volker Hammer, Ulrich Pordesch and Alexander Roßnagel, *Betriebliche Telefon- und ISDN-Anlagen rechtsgemäß gestaltet* (Berlin: Springer, 1993) as a tool for the legally compatible design of ISDN communication systems.

[6] Among others: ubiquitous computing, electronic voting, software agents, multimedia documents, and mobile commerce. For additional reading on the method (in English) see: Alexander Roßnagel and Silke Jandt, "Socially Compatible Technology Design," in *Socio-technical Design of Ubiquitous Computing Systems*, ed. Klaus David, Kurt Geihs, Jan Marco Leimeister, Alexander Roßnagel, Ludger Schmidt, Gerd Stumme, and Arno Wacker (Berlin/Heidelberg: Springer, 2014), 169 ff.; Axel Hoffmann et al., "Towards the Use of Software Requirement Patterns for Legal Requirements," in *2nd International Requirements Engineering Efficiency Workshop (REEW)* 2012 at REFSQ 2012, Essen, Germany.

[7] Cf. the research projects DigiDak (Digitale Daktyloskopie, digital fingerprint identification), CamInSens (distributed smart camera systems) and VASA (Visual Analytics for Security

The method proposed here has been designed to aid decision makers in the selection of legally compatible security measures. However, the aim of the method is not to attach a seal of approval to a certain product that merely indicates conformity with legal minimum requirements; similar to what the CE logo[8] or the ECB-S certificate[9] stand for in the field of product specific conformity. Instead the aim is a qualitative evaluation of the legal compatibility of a security measure beyond minimum requirements. Such a qualitative evaluation allows for a differentiation within the concept of legality as will be shown in the following. The use of the method will then be demonstrated using full body scanners as *one* example of a security measure in public transportation.

3.2 Social and Legal Acceptability of Security Measures

Using full body scanners as an example, this chapter will further illustrate the challenges of the acquisition and implementation of a security measure in a public transportation context that were laid out in the introduction and pinpoint the benefits of increasing the social and legal acceptability of security measures.

From the start, the use of full body scanners in civil aviation has been highly controversial.[10] Their ability to display the naked body beneath the clothes in a very detailed fashion and in high resolution violates many people's sense of decency and shame, and is widely regarded as an intense invasion of privacy. This led to the scanners being nicknamed 'naked scanners' – a term that both pointedly illustrates this issue and serves as a caricature. Body scanners have become the embodiment of (supposedly) exaggerated governmental surveillance and of the perceived security and surveillance ambitions and delusions of governments that followed the events of September 11th 2001. The reason why many rejected and still reject[11] the scanners lies in the fact that a scanner of the so-called first generation actually displayed a

Applications); all sponsored by the German Federal Ministry of Education and Research. The method proposed here has also been introduced into the SIAM FP7 project (Security Impact Assessment Measures – A decision support system for security technology investments, 261826) as part of the Assessment Support Toolkit developed in the project.

[8] Regulation (EC) No. 765/2008 of the European Parliament and of the Council of July 2008 setting out the requirements for accreditation and market surveillance relating to the marketing of products and repealing Regulation (ECC) No. 339/93, L 218/30.

[9] Issued by the European Security Systems Association.

[10] Full body scanners are cabin-like devices for the detection of prohibited objects on a person's body without the need to remove the clothing. The scanners create an image of a person's body using radiation. Depending on the type of radiation used by the scanner, two basic types of scanners can be identified: millimetre wave scanners and X-ray backscatter scanners.

[11] Cf. the ongoing struggle of organisations like the Electronic Privacy Information Center against the use of body scanners in aviation security as an example: http://epic.org/.

visualisation of a person's naked body to the scanner's operator as it was recorded by its sensors. Besides invoking a sense of intrusiveness, this opened the floodgates for voyeuristic abuse.[12]

The producers and end-users reacted with reluctance to the mainly negative reception of the devices. In the United States, the scanners themselves – operated by the Transport Security Administration (TSA) – were not altered at first. Instead, an organisational restructuring occurred. The person analysing the images created by the scanner was now no longer located directly next to the device, but was instead placed in a separate room. The main thought behind this was that voyeurism could be reduced if the person responsible for the analysis of the images could no longer see the person being screened face to face. Only in the second step, the devices themselves were reworked by adding a filter that rendered the faces of the persons being screened unrecognisable.

Both solutions failed to address the concerns voiced against the devices – especially since the devices still displayed pictures of the passengers' naked bodies – and thus proved to be unsatisfactory. In the end the United States began to phase out first generation scanners completely and replaced them with newer, more advanced models of the second generation.[13] The crucial difference between the two generations lies in the fact that second generation devices use software algorithms for the analysis of all images instead of displaying them to a human operator for analysis.[14] When a prohibited item is detected, the display indicates to the human operators where to search the person being screened for the suspected items on an abstracted stick-like representation of the human body. Such items then need to be identified manually by security personnel. In order to realise this, reliable software algorithms had to be developed which are able to take over the job that previously was performed by a human operator, namely the screening for prohibited items carried on a person. It can be asserted that – probably due to time and money constraints – in the first generation a method was chosen that provided

[12] Cf. the following examples: Caroline Black, "Feds Store Body Scans; US Marshals Saved 35,000 Images from Just One Courthouse," CBS News Online, August 5, 2010, accessed September 13, 2013, http://www.cbsnews.com/8301-504083_162-20012785-504083.html; Edecio Martinez and Kevin Hayes, "Penis Jokes Turn TSA Worker Testy; Attacks Co-Worker, Say Police," CBS News Online, May 7, 2010, accessed September 13, 2013, http://www.cbsnews.com/8301-504083_162-20004436-504083.html; Kim Zetter, "Female Passengers Say They Were Targeted for TSA Body Scanners," Wired, February 14, 2012, accessed September 13, 2013, http://www.wired.com/threatlevel/2012/02/female-body-scans/; Michael Holden, "Airport worker warned in scanner ogling claim," Reuters Online, March 24, 2010, accessed September 13, 2013, http://www.reuters.com/article/2010/03/24/us-britain-scanner-odd-idUSTRE62N52E20100324.

[13] Cf. Section 826 of the FAA Modernization and Reform Act of 2010, H.R. 658; U.S. House of Representatives, Committee on Homeland Security, Subcommittee on Transportation Security, *Rebuilding TSA into a Smarter, Leaner Organization*, 113th Congress, September 2012, 11.

[14] The TSA introduced such a software in 2011 under the heading "Automatic Target Recognition". Cf. Department of Homeland Security, *Privacy Impact Assessment Update for TSA Advanced Imaging Technology*, January 25, 2011, http://www.dhs.gov/xlibrary/assets/privacy/privacy-pia-tsa-ait.pdf, 5.

a technologically simpler solution, by having the images screened by a human and not by computer software. When it became clear that the method chosen was unsatisfactory, a purely organisational solution was presented in moving the evaluating personnel away from the scanner. This proved to be inadequate as well. Hence, finally the second generation of body scanners was developed.

In Germany only second generation millimetre wave devices have been used since the technology was introduced to German airports in the context of a field trial. The first generation scanners would arguably not have been fit for use within the German legal system.[15] Apparently, decisive aspects of the use of the technology were not considered during the development process of the first generation, or the legal provisions of one country were taken as a guideline (for example the United States of America) without taking into account that other countries may have different legal provisions for the use of security measures.

This example demonstrates the consequences of technology development that is not in line with social and legal standards and agendas. The added costs for both manufacturers and operators, created by the efforts to mend the technology, could have been avoided if a software solution as realised in the second generation had been implemented from the start. If this had been realised, a substantial amount of the criticism voiced against the first generation would not have come up the first place and it would have been easier to export the devices to other security markets.

This is where a method for the legal evaluation of security measures can come into play. If such a method had been used before purchasing and implementing the scanners, the changes from the first generation to the second that ultimately became necessary could have been anticipated and thus avoided, as well as possible further changes that may become necessary in the future. This would have meant significant cost savings for users and buyers since costly modifications or the refitting of the devices would not have become necessary in the first place. The losses that resulted from the damage to the public image of the scanners, which are difficult to quantify, could have been avoided as well, or at the very least attenuated, since the criticism of the scanners that lead to them being rebranded as ‘naked scanners’ stemmed from the fact that viewing the naked body was not only possible with first generation scanners, it was required.

Acceptance can be an issue for a number of reasons when innovations are introduced. Operators of security products have no interest in investing in a product that may ultimately prove to be useless to them due to legal restrictions or a lack of social acceptance. Adhering to legal requirements can help minimise such issues. Because legal evaluation and social evaluation gear into each other: fundamental

[15] Katalin Busche, “Der Einsatz von Körperscannern auf deutschen Flughäfen: Eine verfassungsrechtliche Bewertung,” *Die Öffentliche Verwaltung* 6 (2011): 225 ff.; Steffen Kroschwald, *Sicherheitsmaßnahmen an Flughäfen im Lichte der Grundrechte* (Kassel: Kassel University Press, 2012), 102 ff. The use of X-ray backscatter scanners in Germany is prohibited by § 25 of the German Radiation Control Regulation (Röntgenverordnung).

rights can be viewed as being expressions of generally accepted social standards and norms. It is thus beneficial to adhere to these fundamental rights when performing an evaluation.

Altering a technology ex post will in many cases be too costly or time-consuming so that it is not a valid option from an economical point of view.[16] In other cases, altering the technology may be impossible altogether. To demonstrate this, body scanners shall once again serve as an example: A user who purchases a body scanner that uses X-radiation has acquired a product that is potentially harmful to health.[17] This basic operating mode cannot be changed. Only the software that the device uses remains modifiable but not its most basic functionality and its harmful side effects.

3.3 The Basic Concepts of Decision Making

This chapter will explore decision making as a process in order to illustrate the underlying chain of thoughts, the problems a decision maker may face and where any form of assistance should be applied, thus laying the foundation for the proposed method for the legal evaluation of security measures. Decision making as a process is defined as the (more or less conscious) choice of one out of several possible alternatives for action.[18] This means that as a basic principle any decision requires a multitude of possibilities and a selection.[19]

The classic decision theories used in business economics are in principle separated into normative and descriptive approaches.[20] An approach is descriptive if it is limited to an empirical analysis, and principles can be derived from this

[16] Alexander Roßnagel, *Rechtswissenschaftliche Technikfolgenforschung: Umrisse einer Forschungsdisziplin* (Baden-Baden: Nomos, 1993), 16 ff.; Gerrit Hornung, *Die digitale Identität: Rechtsprobleme von Chipkartenausweisen* (Baden-Baden: Nomos, 2005), 87 f. In some cases emergency solutions are implemented. One example for this is an ISDN infrastructure without the capability to suppress caller ID. This feature could not be added without significant effort, so the view screens that displayed the telephone numbers of incoming calls were pasted over: Alexander Roßnagel, "Rechtswissenschaftliche Technikfolgenforschung am Beispiel der Informations- und Kommunikationstechniken," in *Technische Innovation und Recht, Antrieb oder Hemmnis?*, ed. Martin Schulte (Heidelberg: C. F. Müller, 1997), 139. Such 'low tech' solutions will however not be possible in most cases and are moreover usually dissatisfactory.

[17] For a list of medical studies of the use of ionising radiation for detection and further references see COM(2010) 311 final, fn. 27. Consequently, only body scanners that do not use ionising radiation may be used in the context of aviation security in the European Union; cf. Chapter 4, 4.1.1.2 d) of the Annex of Regulation (EU) No. 185/2010.

[18] Helmut Laux, Robert Gillenkirch, and Heike Schenk-Mathes, *Entscheidungstheorie* (Berlin/Heidelberg: Springer, 2012), 3.

[19] Niklas Luhmann, *Die Wirtschaft der Gesellschaft* (Frankfurt am Main: Suhrkamp, 1989), 275.

[20] For information on the prescriptive decision theory and the formal decision theory which are also recognized see Susanne Bartscher and Paul Bomke, *Unternehmungspolitik* (Stuttgart: Schäffer-Poeschel, 1995), 54.

analysis.[21] In contrast, normative approaches are aimed at providing assistance for the decision making process. Thus *Laux et al.* write: 'The normative decision theory does not want to describe and explain actual decision making processes, but instead it wants to show how decisions can be made in a rational fashion. It wants to give advice for the solution of decision problems.'[22] The guides for this advice are norms, and not just legal norms, but also for instance social or religious norms.[23] These norms are also aggregates for decisions that impose a burden to make a decision on a person.[24] In the course of an approximation – with the norm as the starting point – a decision maker tries to reach the optimal decision (i.e. the decision that best suits the norms) through the structuring of available alternatives for action; the decision process is divided into stages that finally lead to the dissolution of the pressure of deciding.[25] 'The concern attributed to the normative decision theory is to structure decision problems, to represent them in a formal decision model and to derive from them recommendations for action through logical criteria.'[26] This enables consequent and coherent deductive reasoning which leads to a rational and well-founded decision. Another characteristic of such a model is that it maps out the actual facts of the case in a simplified way. Thus only selected elements of life are introduced into the model.[27] For these reasons, normatively based decisions present the advantage of a methodical framework.[28] The basis of normative decision making is thus the conversion of a concrete decision problem into a formal decision model. The underlying foundation for this is the conception of humans as beings that act and think essentially in a rational way. And while this has come under severe criticism in modern philosophy, it can still be said that – at least in the context of normative decision making – a human being comes to a decision only after weighing alternatives for action. This requires him or her to actually be aware of these alternatives, i.e. a level of information that is as high as possible.[29] Additionally, the decision maker has to have certain objectives that make a rational decision actually possible in the first place.[30]

[21] Bartscher and Bomke, *Unternehmungspolitik*, 54.

[22] Laux, Gillenkirch and Schenk-Mathes, *Entscheidungstheorie*, 4.

[23] These norms however are not just understood as guides in a positive sense, but also in a negative sense as coercion and constraints. Luhmann, *Die Wirtschaft der Gesellschaft*, 284 f. This means for the decision process that it has to be revealed 'which expectations a certain course of decision would violate and whether or not one can want or accept that'. Luhmann, *Die Wirtschaft der Gesellschaft*, 286.

[24] Luhmann, *Die Wirtschaft der Gesellschaft*, 293 f.

[25] Wolfgang Kilian, *Juristische Entscheidung und elektronische Datenverarbeitung* (Frankfurt am Main: Athenäum, 1974), 151.

[26] Bartscher and Bomke, *Unternehmungspolitik*, 54.

[27] Bartscher and Bomke, *Unternehmungspolitik*, 57.

[28] Kilian, *Juristische Entscheidung*, 158.

[29] Michael Bock, *Kriminologie* (München: Vahlen, 2007), para. 177.

[30] Laux, Gillenkirch and Schenk-Mathes, *Entscheidungstheorie*, 18.

It can be hypothesised that there are certain fundamental elements to any decision.[31] Based on these fundamental elements, schemata for any situation imaginable, that requires a decision, can be modelled. The realm of religion, being one of the earliest and pristine norm givers, shall serve as an example to illustrate this: A professing Christian may be faced with a difficult decision in life. From his life situation he isolates those aspects that are relevant to the decision; a step which usually occurs unconsciously. The guideline for his decision is supposed to be the Bible. However, he will not find a passage that corresponds to his concrete situation. He first has to take the fundamental principles which he extracts from the bible[32] and concretise them.[33] Only now can he subsume the facts of the case derived from his life situation under the requirements gathered from the Bible through concretisation; thus knowing what decision to make in order to act in a way that is consistent with the Bible.

A jurist acts in the very same way when subsuming. His norms come from the law. For instance a lawyer seeing a client will first ask the client for a description of the event or the chain of events in question. This description will be given by narration.[34] From the information collected this way he chooses those parts that are relevant to the legal evaluation; these pieces of information form the facts of the case. 'The facts of the case are thus not something that is 'given' or set in advance, but something that has to be composed from the known facts on the one hand and their possible legal significance on the other hand.'[35] From an interpretation of the law the lawyer then chooses the legal requirements, which have to be concretised before finally the facts of the case are subsumed under them. The point thus is 'to assess the case in accordance with the norm; in other words to bring the assessment contained in the norm to bear in a way that corresponds to the case.'[36]

The same thing is true for decision making based on social and other norms.[37] Certain processes that are (perhaps unconsciously) run through by the decision maker can usually be identified. From these processes, the following schema has been derived as an approximation of a universal basis and guideline for normative decision making (Fig. 3.1).

[31] Cf. Laux, Gillenkirch and Schenk-Mathes, *Entscheidungstheorie*, 19 ff.

[32] Examples of such passages are Exodus 20, 2–17; Matthew 5; Marcus 12, 29, 31. The slogan 'What would Jesus do?' which is popular among evangelical Christians also gravitates towards this.

[33] Social ethics, and here especially the Christian social ethics, are concerned with this complex of problems.

[34] Karl Larenz and Claus-Wilhelm Canaris, *Methodenlehre der Rechtswissenschaft* (Berlin/Heidelberg: Springer, 1995), 100.

[35] Larenz and Canaris, *Methodenlehre*, 99.

[36] Larenz and Canaris, *Methodenlehre*, 36.

[37] For example the so-called 'Golden Rule' (regula aurea): 'One should treat others as one would like others to treat oneself.'

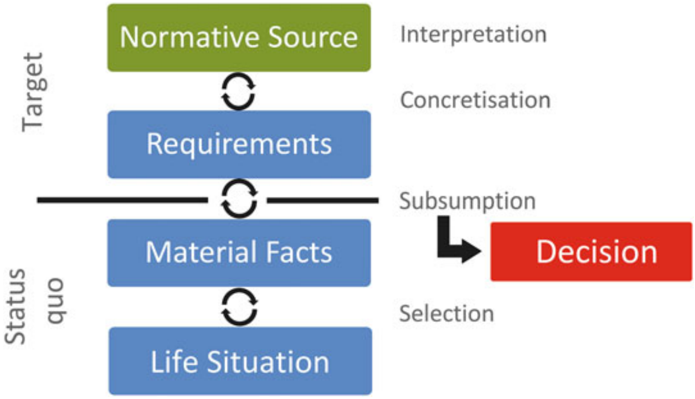


Fig. 3.1 Normative decision making

3.4 The Legal Evaluation of Security Measures

The guidelines presented in this chapter will enable a decision maker to perform a fundamental legal evaluation of existing and future security measures based on the schema distilled in the previous chapter.

Starting point of the evaluation method are the most permanent legal norms, which – through their fundamental and technology neutral nature – provide a framework for future societal developments. Such norms can be found in fundamental rights catalogues. Law below the constitutional level is not suitable as a basis for the method, as it can only be technology neutral to a certain degree.[38] This means that due to the rapid progress of technology it antiquates quickly and thus cannot be used for the compilation of long-lasting guidelines. In addition to this, it is only concerned with a small part of the effects of technology usage.[39] The life expectancy of such subconstitutional laws, especially those concerned with the use of technology, is therefore limited. Fundamental rights and principles however are long-lasting and offer a much more future-proof solution.[40] In addition to this, they serve as guidelines for the interpretation of subconstitutional law.[41] This is true in

[38] Alexander Roßnagel, "'Technikneutrale' Regulierung: Möglichkeiten und Grenzen," in *Innovationen und Recht II: Innovationsfördernde Regulierung*, ed. Martin Eifert and Wolfgang Hoffmann-Riem (Berlin: Duncker & Humblot, 2009), 336 f.; Sabrina Idecke-Lux, *Der Einsatz von multimedialen Dokumenten bei der Genehmigung von neuen Anlagen nach dem Bundesimmissionsschutzgesetz* (Baden-Baden: Nomos, 2000), 213 ff.

[39] Hammer, Pordesch and Roßnagel, *Betriebliche Telefon- und ISDN-Anlagen*, 46.

[40] Roßnagel, *Technikfolgenforschung*, 196.

[41] The rule of constitutionally compatible interpretation demands that from several possible interpretations out of which some would yield a constitutional, some an unconstitutional result,

any legal system based on a hierarchy of norms ('constitutional' statutes versus 'ordinary' statues),[42] as the fundamental rights and principles can be regarded as being the consented objectives of a society.

It is easy to agree that a technology should be socially acceptable. The quarrel begins where it has to be decided what it means exactly to be socially acceptable. But if the definition is based on fundamental rights and principles, which society has already agreed upon as its objectives, consented objectives for a technology design that minimises social conflicts are already predetermined.[43] This underlines the logic behind using fundamental rights and principles as a basis.

However, these fundamental rights and principles do not contain statements that are directly applicable to technical systems.[44] This means that the fundamental rights cannot be the immediate basis for the evaluation and the design of technology; they have to be concretised.[45] This is where the established rules of legal interpretation come into play.[46] As indicated above, the aim is not to ascertain the legality of a technology, but its legal compatibility. Ascertaining the legality of a technology means nothing more than saying that the use of a technology would be legal or illegal within a certain legal framework. In that case, there would be only black and white, which means that this approach is too narrow to provide assistance for a selection process. In contrast, legal compatibility is a broad approach which allows a grading: a technology can be more legally compatible or less legally compatible.[47] It is thus a qualitative approach that allows for a differentiation within the concept of legality. This means that it is not identical with legality and not the opposite of illegality (Fig. 3.2).[48]

those interpretations must be favoured that are constitutionally compatible; BVerfGE 32, 373, 383 f.; Jörn Lüdemann, "Die verfassungskonforme Auslegung von Gesetzen," *Juristische Schulung* 1 (2004): 27 ff.

[42] For the USA cf. the seventh rule of the so-called 'Ashwander Rules'; *Ashwander v. Tennesse Valley Authority*, 297 U.S. 288 (1936), *Crowell v. Benson*, 285 U.S. 22 (1932): 'When the validity of an act of the Congress is drawn in question, and even if a serious doubt of constitutionality is raised, it is a cardinal principle that the Court will first ascertain whether a construction of the statute is fairly possible by which the question may be avoided.'

[43] Alexander Roßnagel, *Allianz von Medienrecht und Informationstechnik?: Ordnung in digitalen Medien durch Gestaltung der Technik am Beispiel von Urheberschutz, Datenschutz, Jugendschutz und Vielfaltschutz* (Baden-Baden: Nomos, 2001), 27.

[44] Hammer, Pordesch and Roßnagel, *Betriebliche Telefon- und ISDN-Anlagen*, 47.

[45] Hammer, Pordesch and Roßnagel, *Betriebliche Telefon- und ISDN-Anlagen*, 46; Roßnagel, *Allianz von Medienrecht und Informationstechnik?*, 29.

[46] The exegesis of a legal norm has to be performed with regard to wording and literal sense (grammatical interpretation), text and systematic structure (systematic interpretation), the will of the lawmaker (historical interpretation) and sense and purpose of the norm (teleological interpretation).

[47] Alexander Roßnagel et al., *Digitalisierung der Grundrechte?: Zur Verfassungsverträglichkeit der Informations- und Kommunikationstechnik* (Opladen: Westdeutscher Verlag, 1990), 7; for a detailed description of this concept see Roßnagel, *Technikfolgenforschung*, 192 ff.

[48] Roßnagel, *Technikfolgenforschung*, 194.

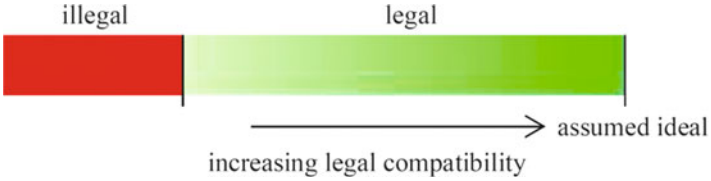


Fig. 3.2 The qualitative approach of the method

When talking about fundamental rights and principles, legal compatibility means compatibility of the underlying social conditions or requirements and of the impact of technological changes with the objectives of the fundamental rights and principles.[49] The term is thus mostly synonymous with social compatibility, as social compatibility is defined as the compatibility with the objectives and standards of a society,[50] whereas the law – and particularly the fundamental rights and principles – is the embodiment and formalisation of these objectives.[51]

By using the means of concretisation of fundamental rights and principles, the method faces the challenge of closing the description gap between broad and unspecific legal requirements – as found for instance in general clauses – and concrete design proposals,[52] because such proposals cannot be found in abstract general clauses.[53] To this end, the general clause, or in this case a fundamental right or principle, is concretised over several steps. Thereby only the legally relevant part of the technology or measure is covered, not the entire functionality.

The outcome of the use of the method can depend on the attitude of its user. This is due to the fact that different interpretations of legal norms exist.[54] This effect can be minimised where the user follows the majority position when faced with a controversial question, especially the rulings of higher courts like the Court of Justice of the European Union. This approach is further advocated by the fact that it strengthens the result of the examination. Still, the use of the method will yield different but congeneric results, varying from user to user. This is a desired

[49] Roßnagel, "Rechtswissenschaftliche Technikfolgenforschung," 148; Roland Steidle, *Multimedia-Assistenten im Betrieb: Datenschutzrechtliche Anforderungen, rechtliche Regelungs- und technische Gestaltungsvorschläge für mobile Agentensysteme* (Wiesbaden: Deutscher Universitäts-Verlag, 2005), 60; Roßnagel, *Technikfolgenforschung*, 26.

[50] Roßnagel, *Technikfolgenforschung*, 193.

[51] Roßnagel, *Technikfolgenforschung*, 194.

[52] Roßnagel, *Technikfolgenforschung*, 16, 28, 67 ff.; Matthias Schwenke, *Individualisierung und Datenschutz: Rechtskonformer Umgang mit personenbezogenen Daten im Kontext der Individualisierung* (Wiesbaden: Deutscher Universitäts-Verlag, 2006), 11; Ulrich Pordesch, *Die elektronische Form und das Präsentationsproblem* (Baden-Baden: Nomos, 2003), 260; Roßnagel, *Allianz von Medienrecht und Informationstechnik?*, 30.

[53] Examples of such abstract general clauses are § 163(1) and 161 of the German Code of Criminal Procedure (Strafprozessordnung; StPO).

[54] Roßnagel, *Technikfolgenforschung*, 198 f.

effect, because the method does not strive to be an automatism, but a guideline that allows for different emphases. The structured composition of the method guarantees traceability. Thus, the results of its use are derived in a clear way and can become a subject for discussion.

The use of the method is composed of four steps. Starting point of its use are the relevant fundamental rights and principles, which have to be identified and selected in a preliminary stage. What follows is a step by step concretisation of the fundamental legal provisions identified in the preliminary stage, at first into legal requirements, then in a second step into legal criteria and in the third step into technical objectives. The abstract legal requirements become more concrete with each step. Between the legal criteria and the technical objectives, a shift occurs from the terminology of the law to the terminology of technology.

As an exception, legal acts below the level of fundamental rights and principles may under certain circumstances also be used as a basis for the method, where they contain direct concretisations of fundamental rights and principles in the form of abstract general clauses.[55] An example of this are the data protection principles found in the European Data Protection Directive.[56] These are concretisations of Article 8 of the Charter of Fundamental Rights of the European Union.

3.4.1 Pre-stage – Identifying Fundamental Legal Provisions

First, in a pre-stage, the relevant fundamental legal provisions as the basis for the evaluation have to be identified. Within the European Union, the catalogues of fundamental rights found in the Charter of Fundamental Rights and in the European Convention on Human Rights can form that basis. Using the Charter as a basis is preferred to using the Convention, since the rights of the Convention are already included in the Charter which itself is based on the Convention. The Charter is more extensive and more up-to-date compared to the 50 year old Convention. It thus makes sense to base an evaluation on the Charter. However, the limits to the legal effect of the Charter have to be kept in mind.

Since the aim of the proposed method is a qualitative evaluation beyond minimum legal requirements, the Charter can serve as a guideline and basis for evaluation even where it is not directly applicable. The use of security measures in the context of aviation security is already subject to the provisions of the Charter.

Another possibility is to use national constitutions as a basis. This is possible wherever a constitution contains a catalogue of fundamental rights.

To be able to reduce such a catalogue of rights to those that are actually relevant for the evaluation, a preliminary evaluation is necessary.

[55] Steidle, *Multimedia-Assistenten im Betrieb*, 62.

[56] 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, L 281/31.

3.4.1.1 Type and Functions of the Security Measure

At the beginning of the evaluation, a certain security measure will have been selected for evaluation, based most likely on criteria like effectiveness in providing security and overall costs. This means that the very start of the procedure is the decision in favour of a certain measure, for instance a system for biometric access control or video surveillance.

To make this decision in a professional way, at the very least some basic technological knowledge, as well as knowledge in the fields of security and counter-terrorism are required. Here scenarios and scenario building tools can be helpful, as they give indications for the necessity and suitability of a measure. The second pillar of decision making in this context are the technological and social features of a security measure. Ideally, the decision maker should rely on more than his or her own expertise, but consult other experts and gather second opinions in order to ensure that the facts gathered in this phase of the evaluation are sufficiently robust.

At the end of this step, type and functions of the security measure that is to be evaluated will be identified.

3.4.1.2 Fundamental Legal Provisions

After the basic functions of a measure have been isolated and carved out, the fundamental legal provisions can be identified. To do this, it is necessary for the user to possess legal knowledge. A fundamental right or principle is relevant, if its protected sphere is affected by the measure being evaluated. Furthermore, a fundamental right can become relevant where it is facilitated by the measure. To determine this, the chances and risks of the use of the security measure relative to the exercise of fundamental rights and principles have to be examined. These chances and risks are derived from the functions identified in the previous step. This is in line with the target to extract legal requirements from social principles that are the basis for legal norms. Depending on type and functions of a security measure, different fundamental rights will be affected.

It has to be noted that the goals stated in fundamental rights do not just stand side by side, but that they often come in conflict with each other, meaning there are conflicts of goals.[57] Such conflicts can occur in every stage of the method. They should not be solved immediately if possible, but instead be carried on as far as possible in order not to lose alternative solutions that may result from these conflicts of goals. This enables the user of the proposed method to balance different fundamental rights issues in the final stage of the use of the method (e.g. issues relating to human dignity, bodily integrity, privacy and so forth) and even to put an emphasis on the resolution of one issue in favour of another when ultimately choosing a security measure. The method is not meant to impose on the user which

[57] Roßnagel, *Technikfolgenforschung*, 200.

	LP #1	LP #2	LP #3	…
F #1	✓	✓	✓	
F #2	-	✓	-	
F #3	✓	-	✓	
…				

✓ shows, that a function (F) affects the protected sphere of a fundamental legal provision (LP)

Fig. 3.3 Example of a diagram of the functions of a security measure and the affected fundamental rights

fundamental right is more important in case of a conflict, and indeed it cannot do so since the answer depends on the individual case at hand. Instead, the additional value of the use of the method in regard to conflicts is that its use will reveal the existence of such conflicts and uncover alternative solutions for individual fundamental rights issues. By revealing conflicts, the method helps to prevent and correct any one-dimensional maximisation of an individual target value.[58]

The carved out functions and the fundamental legal provisions should be linked in a table in order to increase clarity and traceability of the process (Fig. 3.3).

3.4.2 Stage 1 – Deduction of Legal Requirements

What follows is the first step of the concretisation process in which the fundamental legal provisions are condensed and channelled into legal requirements. Where such concretisations already exist, for example in the shape of a court ruling, they can be resorted to. In any other case, the conventional methods of legal interpretation should be used.[59]

The legal requirements are the product of the legal interpretation of social functions that are affected by the technology being evaluated. This makes it necessary to establish a relation between the fundamental legal provisions and the social functions of the technology.[60] The goal of this first step of the use of the method is to create legal norms that have been specified for the technological environment. The legal requirements are expressed in legal terminology.

Two important aspects have to be kept in mind from the very start of the use of the proposed method:

The principle of proportionality[61] can neither serve as a fundamental legal provision nor as a requirement; rather it is an implicit part of the method. This

[58] Hammer, Pordesch and Roßnagel, *Betriebliche Telefon- und ISDN-Anlagen*, 86.

[59] Cf. fn. 46.

[60] Pordesch, *Die elektronische Form*, 266 f.

[61] As found in Article 52(1) of the Charter of Fundamental Rights of the European Union.

results from the fact that the question of the proportionality of a measure – and thus of the material lawfulness – is an aspect of legal compatibility, which aims at a gradation of proportionality. Proportionality is thus not located on the level of legal requirements, but instead it is an overarching concept that lances the evaluation as a whole and which is ultimately absorbed by the concept of legal compatibility.

The method does not restrict the evaluation to technological aspects of a security measure. Instead, organisational aspects have to be considered as well during the use of the method. This results from the fact that a security measure that has been acquired as a result of a positive evaluation then has to be implemented. This implementation – the organisational design of the newly acquired security measure – is equally important for the realisation of fundamental rights as the technological design of the measure, since a measure could be designed in a way to respect fundamental rights very well, but then be implemented in a way that negates this, e.g. through abusive security staff. It is of paramount importance to derive organisational solutions to fundamental rights issues *together* with the technological solutions since a security measure may be designed in a way that makes it impossible to realise a certain organisational requirement or that would make significant alterations necessary. Therefore, a decision maker has to be aware of these organisational solutions before a decision is made in favour of a certain security measure.

3.4.3 Stage 2 – Concretisation into Legal Criteria

The legal requirements are now concretised into legal criteria by deriving from the legal requirements the basic requisites concerning the use of the security measure. In order to do this, rules have to be identified which determine how to fulfil the legal requirements with regard to the specific features, risks and conditions of the use of the security measure.[62] The criteria thus derived are both connected to the technology as well as to the social and legal aspects. They are the bridge between the law and technology and herald a change in terminology from the legal terminology to the terminology of technology. This means that while the language used becomes more and more technical during the process of concretisation, the legal criteria form the threshold between legal terminology and technical terminology.

Legal criteria describe solutions for the problems within the legal requirements, but without a limitation to a certain concrete technological, organisational or legal approach. All technical and non-technical possibilities for solutions still remain possible at this stage.[63]

[62] Hammer, Pordesch and Roßnagel, *Betriebliche Telefon- und ISDN-Anlagen*, 46.

[63] Pordesch, *Die elektronische Form*, 261.

3.4.4 Stage 3 – Concretisation into Technical Objectives

On the third stage, technical objectives are derived from the legal criteria by looking for the most basic functions that the technology has to have in order to fulfil the demands set by the legal criteria. Since they can also contain organisational objectives that do not pertain to the concrete design of a technology, but rather to the environment and manner of its use, they could also more accurately be called technical and organisational objectives. The technical objectives are abstractions of concrete technological features. The concretisation of legal criteria is based on considerations about how to transform these legal criteria into basic functions of a security measure including organisational aspects. The objectives thus developed are descriptions of functions and technical requirements in general terms.

On this stage, alternative proposals can be developed to have a broader basis for the comparison following in the final stage. Such alternative proposals can also facilitate a comparison between several security measures that try to give different solutions to legal requirements.

The objectives derived should indicate how to best adhere to fundamental legal provisions. This means that they will often go beyond minimum legal requirements and it also means that conflicts between objectives will arise. The security measure that is ultimately chosen by the decision maker should be the one that best fulfils the technical objectives and that best strikes a proper balance between conflicting objectives.

3.4.5 Stage 4 – Comparison

The use of the method concludes with a comparison of security products with the technical objectives developed in the previous stage. If the user evaluates more than one security measure, he or she is advised to draft a table containing an overview as shown in Fig. 3.4. Alternatively, the technical objectives can be used as a checklist for the selection of a suitable security measure. It has to be kept in mind

	SM #1	SM #2	SM #3	...
TO #1	☺	☹	☹	
TO #2	☹	😐	☺	
TO #3	☺	☺	☺	
...				

A security measure (SM) fulfils a technical objective (TO) completely (☺), partially (😐) or not at all (☹).

Fig. 3.4 Example of a diagram when comparing security measures

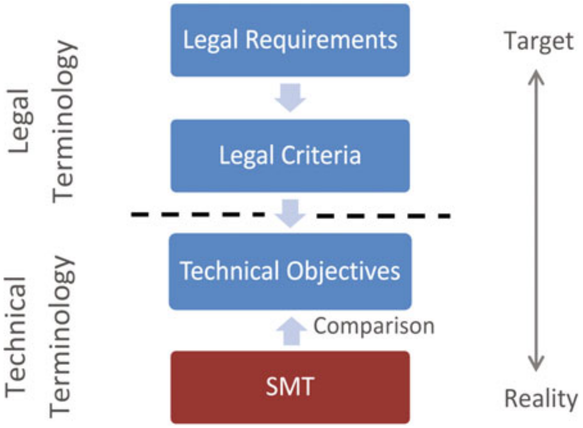


Fig. 3.5 A method for the legal evaluation of security measures; *SMT* Security Measure or Technology

that it is possible for a security measure to only partially comply with a technical objective. Also, when comparing several security measures, the situation can occur that a number of candidates are equally compatible with technical objectives. In such a case the user should fall back to non-legal factors to decide between these candidates.

After a security product has been purchased, the organisational objectives which have been developed in stage 3 as a side-product come into play, as well as technical objectives which take a dual function by containing both purely technological and purely organisational aspects. They give advice to the decision maker how to implement the new security measure and which organisational structure surrounding the measure he or she should choose.

For a summary illustration of the structure of the method see Fig. 3.5.

3.4.6 *Alternative: Stage 4 – Technical Design Proposals*

As an alternative to stage 4 as described above, the technical objectives that have been developed over the course of the use of the method can be further refined into technical design proposals.[64] Thus, the method can be of interest not just to end users of security measures, but also to manufacturers and developers in the security sector that want to benefit from the continuous boom in demand, by enabling them to develop security products that are legally compatible and that hence can survive

[64] In this context, design means any purposeful development and alteration of technical systems; cf. Roßnagel, "Rechtswissenschaftliche Technikfolgenforschung," 267 f. The normative design approach that this method is based on has to be differentiated from design based on empirical observations.

in the marketplace and prevail in the critical eyes of the public. Furthermore, end-users can use the design proposals to demand improvements and reworking of a product from its manufacturer; thus exerting influence on the technological design of a security measure.

Technical design proposals are a collection of measures for direct implementation into the technology.[65] They are often not without alternatives; they should be seen as proposals, as their name indicates. This means that, just as the technical objectives, the catalogue of measures created in this last step can contain several alternative solutions for an individual problem. This is due to the fact that the aim is not to create a coherent system design. In fact this cannot be the case as the method only looks at those aspects of a technology that are legally relevant. However, the proposals developed should be fit for direct implementation. This means that they have to be concrete enough that they could become part of a technical specifications sheet.[66] Their implementation may not be strictly necessary from a legal point of view, but it should at least be desirable. This is due to the fact that the results of the use of the method have been designed to fulfil fundamental legal provisions in the best way possible which means that they can be above the legally required minimum standard.[67]

During the creation of a technology, the technicians, engineers, etc. involved can work towards the implementation of these measures. The method would then come into play during the design phase of technology development, after a technology has been defined beyond the early stages of conceptual development.[68] This means that there already has to be some idea about composition and capabilities of a technology, i.e. ideally after an early prototype has been constructed.

If the method is used in this context, those technical objectives which are not strictly concerned with technology design, but rather with the use of technology and its organisation, must not be omitted; they remain relevant. Already in the early stages of the design process it has to be made sure that technology is designed in a way that does not hinder or preclude certain legally compatible organisational options.

A good example of this would be a hypothetical technical objective that demands that the person evaluating images created by a body scanner is located out of sight of the scanner. If the manufacturer does not implement the capability to transmit the images to another location (and if this feature cannot be added later), then security

[65] Philip Laue, *Vorgangsbearbeitungssysteme in der öffentlichen Verwaltung: Rechtliche Rahmenbedingungen und Gestaltungsanforderungen* (Kassel: Kassel University Press, 2010), 65.

[66] Pordesch, *Die elektronische Form*, 267 f. A definition of what is meant by a technical specifications sheet (Lastenheft) can be found in DIN 69905.

[67] Katharina Bräunlich et al., “Verbindung von CC-Schutzprofilen mit der Methode rechtlicher IT-Gestaltung KORA,” *Datenschutz und Datensicherheit* 2 (2011): 130.

[68] Volker Hammer et al., *Vorlaufende Gestaltung von Telekooperationstechnik: am Beispiel von Verzeichnisdiensten, Personal Digital Assistants und Erreichbarkeitsmanagement in der Dienstleistungsgesellschaft* (Sankt Augustin: Gesellschaft für Mathematik und Datenverarbeitung mbH, 1994), 4, 6 f.; Steidle, *Multimedia-Assistenten im Betrieb*, 64.

personnel evaluating the images can only be situated directly at the device; thus making it impossible to implement the objective.

Quite the contrary, producers should work towards promoting certain organisational options which benefit fundamental rights. To that end, it is imperative that producers concern themselves with organisational aspects and possibilities of the later use on the level of technical objectives and design proposals, and account for them in the development process. Fundamental rights would benefit even more, if producers were to pass recommendations for the implementation of their products and its organisational environment on to the buyers and users. In order to realise this, it is again necessary for producers to concern themselves actively with these aspects.

If used during the development of a security measure, the aim and effect of the method is avoiding or at least minimising the immanent risks of a technology before introducing a product to the market. Risk in this context means any negative effect or impact that a technology might have. Another aim is the achievement or strengthening of chances, meaning positive consequences.[69]

3.4.7 Example of Use

As was shown above, body scanners are a highly controversial technology. This means that they are well suited to provide a short and simplified example of the use of the methodology proposed in this chapter.

The basic functionality of a body scanner can be summarised as follows. A body scanner:

- irradiates the body with electromagnetic radiation,
- penetrates clothing,
- creates an image of the naked human body, and
- detects objects hidden on the body and in clothing.

Fundamental rights and principles of the Charter of Fundamental Rights of the European Union affected by the use of full body scanners – derived from the chances and risks behind the technology – are:

- Article 1 CFR – Human dignity,
- Article 3(1) CFR – Right to the integrity of the person,
- Article 4 CFR – Prohibition of torture and inhuman or degrading treatment,
- Article 7 CFR – Respect for private and family life,
- Article 8(1,2) CFR – Protection of personal data,
- Article 10(1) CFR – Freedom of thought, conscience and religion,
- Article 21(1) CFR – Non-discrimination,
- Article 24(2) CFR – The rights of the child,

[69] Christoph Schnabel, *Datenschutz bei profilbasierten Location Based Services: Die datenschutzadäquate Gestaltung von Service-Plattformen für Mobilkommunikation* (Kassel: Kassel University Press, 2009), 32; Pordesch, *Die elektronische Form*, 257.

- Article 25 CFR – The rights of the elderly,
- Article 26 CFR – Integration of persons with disabilities,
- Article 35 CFR – Health care, and
- The rule of law.[70]

A complete evaluation would go beyond the scope of this contribution. The following is an excerpt of how such an evaluation would look like.[71] The information above forms the basis of the evaluation and is a summary of the results of what would happen in the pre-stage of the evaluation.

The underlying scenario shall be the planned introduction of full body scanners at a European airport. For the first example, Article 35 CFR has been selected to demonstrate the different steps of concretisation from fundamental legal provisions to legal requirements, to legal criteria and ultimately to technical objectives. The second example will show how conflicts emerge and how to deal with them. Finally, the third example will give an instance of the derivation of an objective that is concerned with organisational aspects.

3.4.7.1 Example No. 1

Article 35 in conjunction with Articles 3(1) and 24(2) CFR as fundamental legal provisions can be concretised into the legal requirement 'harmlessness to health': It has to be made sure that the use of the scanner is in no way hazardous to the health of the passengers being screened as well as to the health of the operating personnel and other personnel. When evaluating possible health risks, dissenting medical opinions and minority opinions should also be taken into account. A technology may only be used when there is a broad consensus in medical and biological research on its lack of risks.

In the next step, this legal requirement could be concretised into the legal criterion 'protection from radiation': Even where no direct health risks are scientifically proven, in the interest of risk prevention it should be demanded that the emission of radiation is reduced to a minimum in order to counteract possible long term effects on health that are yet unknown. The lower limit for this reduction is the threshold beyond which reliable detection is no longer possible, thus threatening the proper functioning of the scanner.

[70] The rule of law is mentioned in the preamble of the Charter as one of the principles that the European Union is based on. The rule of law is furthermore postulated by the citizens' rights contained in chapter V and the judicial rights found in chapter VI of the Charter. Jürgen Meyer, *Charta der Grundrechte der Europäischen Union* (Baden-Baden: Nomos Kommentar, 2011), Präambel GRCh, para. 9, 34.

[71] An exhaustive example based on the body scanner technology can be found in Geminn, *Rechtsverträglicher Einsatz von Sicherheitsmaßnahmen im öffentlichen Verkehr*, 369 ff. In this exemplary evaluation, all in all 11 legal requirements have been converted into 19 legal criteria and 20 technical objectives, most of which interact.

In the following step, this legal criterion could be further refined into the technical objective 'no harmful exposure to radiation' amongst others. This means that ionising radiation must not be used, which bars scanners based on X-radiation from being used; including devices that operate with very low dosages. This is consistent with Commission Regulation (EU) No. 185/2010.[72] When using millimetre wave scanners and Terahertz scanners, limit values for radiation must be adhered to. The scan method that is most harmless from a medical point of view and that offers the lowest radiation exposure levels should take precedence. This means that the use of a passive scan method should in principle be privileged.

In the final stage of the method, together with the other technical objectives derived through the use of the method, this technical objective would have to be compared to body scanners available for purchase.

3.4.7.2 Example No. 2

The Rule of Law[73] can be concretised into the legal requirement 'prohibition of unnecessary interference'. The requirement prohibits any design or use of a body scanner in a way that results in unnecessary interference and imposition. This prohibition is first of all a requirement concerning the operational capabilities and the performance of the scanner. Where software is used for analysis of the images, it must not mistake harmless objects, items and features for dangerous ones. Where the images are analysed and evaluated by a human operator, the image displayed must be of sufficient quality to enable the operator to distinguish objects in a reliable way. Furthermore, the prohibition of unnecessary interference can serve as an argument that can be brought forward in favour of the use of analysis software over the analysis of the images created by the scanner through human personnel. The reasoning behind this is that where software is used, intimate facts and features that are not relevant to security as well as the shape of one's body is only registered by the device, but not by a human being.

In the next step, this legal requirement could be concretised into the legal criterion 'rate of false positives/selection of suspicious features' amongst others: From the prohibition of unnecessary interference result specifications for the rate of false positives and thus for the selection of features that during the evaluation and analysis of the images – be it by human personnel or by software – are assessed as being suspicious or relevant to security, meaning that they will give rise to further investigation. Neither human personnel nor software must be allowed to mistake a

[72] Commission Regulation (EU) No. 185/2010 of 4 March 2010 laying down detailed measures for the implementation of the common basic standards on aviation security, L 55/1. Cf. Chapter 4, 4.1.1.2 d) of the Annex of Regulation (EU) No. 185/2010; additionally see Part A Section 1 Subsection 2 f) of Commission Regulation (EC) No. 272/2009.

[73] See fn. 70.

medical aid like an artificial anus for a hidden weapon. This criterion is thus both a performance requirement for the technology as well as for the human operators.

In the following step, this legal criterion could be further refined into the technical objective 'handling of false positives' amongst others: Those software algorithms have to be chosen that produce the lowest amount of false positives possible. This is to avoid that persons are in the course of the investigation of a false positive subjected to pat-downs, searches and questioning without having given reason for this. At the same time, the intensity of the radiation has to be regulated in accordance with this. As a general rule, a greater emission of radiation will produce a higher detection capability which will in return reduce the amount of false positives. Thus, a conflict arises with the technical objective developed in the first example which demands the lowest possible emission of radiation in order to avoid any risks to passengers' health.

As in the first example, the final stage is the comparison of the technical objective that has been derived with body scanners available for purchase. While also keeping other objectives in mind that would have been derived in a complete evaluation, the user of the method should choose the device that best strikes the balance between the technical objectives. Where a device allows for the adjustment of the emission, the decision maker has to balance the two conflicting technical objectives.[74]

3.4.7.3 Example No. 3

Articles 7 and 8(1,2) CFR can be concretised into the legal requirement 'informational self-determination'. Informational self-determination means the freedom from unlimited collection, storage, use and dissemination of personal data and it guarantees the authority of each individual to decide in principle for him- or herself whether or not to reveal personal data and thus to decide when and under what circumstances to disclose facts of life.

Among others, the legal criterion 'transparency' can be derived from this legal requirement: A passenger can only realise his or her data protection rights if he or she possesses information about the body scanner and the organisational aspects surrounding its use. Thus the operator of the scanner has to ensure transparency. This relates to the collection, processing and use of personal data, but is not limited to these aspects. Rather, there should be transparency concerning all information relevant to the realisation of relevant legal rights. It has to be kept in mind that information has to be devised and prepared in such a way that it can be understood without the help of technicians or other experts. Furthermore, the information has to be designed in a way that it can be captured at a glance if possible, while taking

[74] Using X-ray backscatter scanners as an example, *Cao* illustrates how such a complex weighing can look like: Zongjian Cao, "Optimization for the tradeoff of detection efficiency and absorbed dose in x-ray backscatter imaging," Journal of Transportation Security 1 (2013), 59 ff.

language barriers into account. Thus, the imperative of transparency is foremost an organisational measure that accompanies the operation and use of the scanner.

In the following step the technical objective ‘informing passengers’ can be derived from this criterion. Passengers that go through the scanner have to be informed about the technical features of the scanner and the organisational framework of its use. This is the only way passengers can make an informed decision whether or not to go through the scanner. This is consistent with the requirements of Commission Regulation (EU) No. 185/2010: ‘Before being screened by a security scanner, the passenger shall be informed of the technology used, the conditions associated to its use and the possibility to opt out from a security scanner.’[75] Keeping in mind that the aim of the proposed method is to accommodate fundamental rights in the best way, merely informing passengers on demand does not fully satisfy the objective. Informing passengers should happen actively. Personally informing every single passenger by human personnel will most likely be too costly and time-consuming. What remains is the possibility to educate by the use of signs or monitors. It must be pointed out that – besides information about the basic functions and features of the scanners – there should also be directions on prohibited items and alternative control measures. This is due to the fact that the passenger must be aware of all relevant basic parameters in order to enable an informed decision.

As indicated above, the focus of this objective lies on organisational aspects of the use of body scanners. It will thus have to play in important role during the process of implementation.

Generally speaking, with objectives that concern organisational aspects, the decision maker should check at the comparison stage whether or not a device has the technical capability to conform to the objective. A decision maker should at this point also check whether or not his facility can accommodate the objective in an organisational sense, e.g. check if there is enough staff or equipment available.

3.5 Summary and Conclusion

This paper has attempted to demonstrate both the need for and the feasibility of a systematic approach to the legal evaluation of security measures. The method which has been presented aids in the process of evaluating the legal compliance of security measures, but it also advertises and encourages decision makers to go beyond the bare minimum of what is legally required. Using fundamental rights and principles which can be found not only in the Charter of Fundamental Rights but also in most national constitutions as a basis confronts decision makers with these rights and principles and helps to promote them. At the same time, using them as a basis ensures the longevity of the validity of any decision made using the method, all while increasing the social acceptability of the decision.

[75] Annex Chapter 4 Section 4.1.1.10.

The proposed method sets itself apart from other methods and particularly from privacy impact assessment (PIA) through certain distinct characteristics. A PIA 'is a methodology for assessing the impacts on privacy of a project, policy, programme, service, product or other initiative which involves the processing of personal information and, in consultation with stakeholders, for taking remedial actions as necessary in order to avoid or minimize negative effects'.[76] The methodology employed in PIAs 'differs from one regime to another, from one company to another'[77] and PIAs have in the past 'been performed in a highly variable way'.[78] This complicates a direct comparison of the proposed method and PIAs.

First of all, the method does not limit the evaluation to certain aspects like privacy (PIA) or data protection (data protection impact assessment, DPIA). Instead, all fundamental rights that are affected by a security measure are introduced into the evaluation, meaning that the approach of the method is holistic by default. At the core of most PIA methodologies lies a series of open and closed questions.[79] The answers to these questions as well as the questions themselves are meant to raise awareness of privacy issues and to help find suitable solutions to these issues.[80] The proposed method however is founded on the step by step concretisation of fundamental rights which consequently form the starting point of the use of the method. Herein lies the main advantage of the proposed method: The use of the method is closely tied to an evaluation of the impact of a certain security measure on fundamental rights. Through the process of concretisation, the derived results retain their close link to fundamental rights, while being transformed into much more 'technology-compatible' terminology. This addresses some of the common deficiencies in PIAs which *Wright* and *De Hert* cite – among others – as: 'seeing the PIA process as a legal compliance audit; the failure to link identified risks with the specific design elements of a project; and the proposed mitigating measures often not appropriate to the risks identified', as well as the challenging nature of the 'implementation of reported findings'.[81] In contrast, the proposed method aims to illustrate how to bring fundamental rights to life in the best possible way. This qualitative approach of the method – together with a concretisation towards

[76] David Wright and Paul De Hert, "Introduction to Privacy Impact Assessment," in *Privacy Impact Assessment*, ed. David Wright and Paul De Hert (Dordrecht: Springer, 2012), 5. For a comprehensive list of literature on PIA see Information Commissioner's Office, *Conducting privacy impact assessments: code of practice* (London: ICO, 2014), 42 f.

[77] Wright and De Hert, "Introduction to Privacy Impact Assessment," 6.

[78] David Wright and Paul De Hert, "Findings and Recommendations," in *Privacy Impact Assessment*, ed. David Wright and Paul De Hert (Dordrecht: Springer, 2012), 479.

[79] See for example Information Commissioner's Office, *Conducting privacy impact assessments*, 33; Department of Homeland Security, *Privacy Impact Assessments: The Privacy Office Official Guidance* (Washington, DC: DHS, 2010), 14 ff.

[80] Wright and De Hert, "Findings and Recommendations," 473: "Questions feature in virtually all PIA methodologies as a way of stimulating consideration of the issues raised by a new technology, service or policy."

[81] Wright and De Hert, "Findings and Recommendations," 479.

the terminology of technology – also facilitates the direct comparison of certain brands and models of security measures. The high variance in quantity and quality of PIA outcomes is addressed by the fact that with the proposed method the expenditure automatically scales depending on the intrusiveness and the expected benefits of the security measure being evaluated, since – with fundamental rights being the starting point of the use of the measure – the count of affected fundamental rights and the quality of the impact of a measure on an individual fundamental right determine the extent of the foundation that the evaluation is based upon. In addition to this, the proposed method offers a more formalised framework while still retaining the necessary flexibility. Furthermore, the method promotes interdisciplinary cooperation as an individual user will often have to rely on expert opinions and an exchange of knowledge during the process of concretisation, for instance to be able to evaluate medical hazards or social impact.

The proposed method is meant for the evaluation of security measures available for purchase, which includes aiding in the implementation of security measures and the design of their organisational framework. However, the paper also emphasised the need to incorporate legal requirements early during the design process of new security measures. In practice, development of new technologies usually takes place without taking into account human rights aspects of the use of the final product, and instead focuses on functional efficiency and serviceability.[82] Designing technologies is a process characterised by the selection of individual design choices. Throughout the process of technology genesis and development, decisions have to be made and their impacts, including legal impacts, have to be evaluated. The method, used as a rule-based approach for the normatively guided design of technology, can also support developers by helping them choose those design options that are best suited to fulfil legal requirements. If used in this way, the method shares a common approach with PIA in that it has to come into play during the early life of a project and in that it should run alongside the project as an iterative process.

References

Bartscher, Susanne, and Paul Bomke. *Unternehmungspolitik*. Stuttgart: Schäffer-Poeschel, 1995.

Bock, Michael. *Kriminologie*. München: Vahlen, 2007.

Bräunlich, Katharina, Philipp Richter, Rüdiger Grimm, and Alexander Roßnagel. “Verbindung von CC-Schutzprofilen mit der Methode rechtlicher IT-Gestaltung KORA.” *Datenschutz und Datensicherheit* 2 (2011): 129.

Busche, Katalin. “Der Einsatz von Körperscannern auf deutschen Flughäfen: Eine verfassungsrechtliche Bewertung.” *Die Öffentliche Verwaltung* 6 (2011): 225.

Cao, Zongjian. “Optimization for the tradeoff of detection efficiency and absorbed dose in x-ray backscatter imaging.” Journal of Transportation Security 1 (2013): 59.

Department of Homeland Security. *Privacy Impact Assessments: The Privacy Office Official Guidance*. Washington, DC: DHS, 2010.

[82] Steidle, *Multimedia-Assistenten im Betrieb*, 55.

Geminn, Christian Ludwig. *Rechtsverträglicher Einsatz von Sicherheitsmaßnahmen im öffentlichen Verkehr*. Wiesbaden: Springer Vieweg, 2014.

Hammer, Volker, Ulrich Pordesch and Alexander Roßnagel. “KORA, Eine Methode zur Konkretisierung rechtlicher Anforderungen zu technischen Gestaltungsvorschlägen.” *Infotech/I + G* 1 (1993): 21.

Hammer, Volker, Ulrich Pordesch, and Alexander Roßnagel. *Betriebliche Telefon- und ISDN-Anlagen rechtsgemäß gestaltet*. Berlin: Springer, 1993.

Hammer, Volker, Ulrich Pordesch, Alexander Roßnagel, and Michael Schneider. *Vorlaufende Gestaltung von Telekooperationstechnik: am Beispiel von Verzeichnisdiensten, Personal Digital Assistants und Erreichbarkeitsmanagement in der Dienstleistungsgesellschaft*. Sankt Augustin: Gesellschaft für Mathematik und Datenverarbeitung mbH, 1994.

Hoffmann, Axel, Thomas Schulz, Holger Hoffmann, Silke Jandt, Alexander Roßnagel and Jan Marco Leimeister. “Towards the Use of Software Requirement Patterns for Legal Requirements.” In *2ndInternational Requirements Engineering Efficiency Workshop (REEW)* 2012 at REFSQ 2012, Essen, Germany.

Hornung, Gerrit. *Die digitale Identität: Rechtsprobleme von Chipkartenausweisen*. Baden-Baden: Nomos, 2005.

Idecke-Lux, Sabrina. *Der Einsatz von multimedialen Dokumenten bei der Genehmigung von neuen Anlagen nach dem Bundesimmissionsschutzgesetz*. Baden-Baden: Nomos, 2000.

Information Commissioner’s Office. *Conducting privacy impact assessments: code of practice*. London: ICO, 2014.

Kilian, Wolfgang. *Juristische Entscheidung und elektronische Datenverarbeitung*. Frankfurt am Main: Athenäum, 1974.

Kroschwald, Steffen. *Sicherheitsmaßnahmen an Flughäfen im Lichte der Grundrechte*. Kassel: Kassel University Press, 2012.

Larenz, Karl, and Claus-Wilhelm Canaris. *Methodenlehre der Rechtswissenschaft*. Berlin/Heidelberg: Springer, 1995.

Laue, Philip. *Vorgangsbearbeitungssysteme in der öffentlichen Verwaltung: Rechtliche Rahmenbedingungen und Gestaltungsanforderungen*. Kassel: Kassel University Press, 2010.

Laux, Helmut, Robert Gillenkirch, and Heike Schenk-Mathes. *Entscheidungstheorie*. Berlin/Heidelberg: Springer, 2012.

Luhmann, Niklas. *Die Wirtschaft der Gesellschaft*. Frankfurt am Main: Suhrkamp, 1989.

Lüdemann, Jörn. “Die verfassungskonforme Auslegung von Gesetzen.” *Juristische Schulung* 1 (2004): 27–30.

Meyer, Jürgen. *Charta der Grundrechte der Europäischen Union*. Baden-Baden: Nomos Kommentar, 2011.

Pordesch, Ulrich. *Die elektronische Form und das Präsentationsproblem*. Baden-Baden: Nomos, 2003.

Roßnagel, Alexander. *Rechtswissenschaftliche Technikfolgenforschung: Umrisse einer Forschungsdisziplin*. Baden-Baden: Nomos, 1993.

Roßnagel, Alexander. “Rechtswissenschaftliche Technikfolgenforschung am Beispiel der Informations- und Kommunikationstechniken.” In *Technische Innovation und Recht, Antrieb oder Hemmnis?*, edited by Martin Schulte, 139–162. Heidelberg: C. F. Müller, 1997.

Roßnagel, Alexander. *Allianz von Medienrecht und Informationstechnik?: Ordnung in digitalen Medien durch Gestaltung der Technik am Beispiel von Urheberschutz, Datenschutz, Jugendschutz und Vielfaltschutz*. Baden-Baden: Nomos, 2001.

Roßnagel, Alexander. “‘Technikneutrale’ Regulierung: Möglichkeiten und Grenzen.” In *Innovationen und Recht II: Innovationsfördernde Regulierung*, edited by Martin Eifert and Wolfgang Hoffmann-Riem, 323–327. Berlin: Duncker & Humblot, 2009.

Roßnagel, Alexander, and Silke Jandt. “Socially Compatible Technology Design.” In *Sociotechnical Design of Ubiquitous Computing Systems*, edited by Klaus David, Kurt Geihs, Jan Marco Leimeister, Alexander Roßnagel, Ludger Schmidt, Gerd Stumme, and Arno Wacker, 169–182, Berlin/Heidelberg: Springer, 2014.

Roßnagel, Alexander, Peter Wedde, Volker Hammer, and Ulrich Pordesch. *Digitalisierung der Grundrechte?: Zur Verfassungsverträglichkeit der Informations- und Kommunikationstechnik*. Opladen: Westdeutscher Verlag, 1990.

Schnabel, Christoph. *Datenschutz bei profilbasierten Location Based Services: Die datenschutzadäquate Gestaltung von Service-Plattformen für Mobilkommunikation*. Kassel: Kassel University Press, 2009.

Schwenke, Matthias. *Individualisierung und Datenschutz: Rechtskonformer Umgang mit personenbezogenen Daten im Kontext der Individualisierung*. Wiesbaden: Deutscher Universitäts-Verlag, 2006.

Steidle, Roland. *Multimedia-Assistenten im Betrieb: Datenschutzrechtliche Anforderungen, rechtliche Regelungs- und technische Gestaltungsvorschläge für mobile Agentensysteme*. Wiesbaden: Deutscher Universitäts-Verlag, 2005.

Wright, David, and Paul De Hert. “Introduction to Privacy Impact Assessment.” In *Privacy Impact Assessment*, edited by David Wright and Paul De Hert, 3–32, Dordrecht: Springer, 2012.

Wright, David, and Paul De Hert. “Findings and Recommendations.” In *Privacy Impact Assessment*, edited by David Wright and Paul De Hert, 445–481, Dordrecht: Springer, 2012.

Chapter 4
Models and Tools for the Computational Support of Technology Impact Assessments, Applied in the Context of Mass Transportation

Ronald R. Grau

Abstract This chapter describes the conceptual and practical developments for a software prototype created in the course of the SIAM FP7 project (EC reference 261826). The term assessment support system was coined to characterise this system because its inherent aim is to provide insight about the assessment process itself and so enhance, rather than replace, traditional decision support approaches. An assessment support system follows a participative, human-driven approach and takes as input the specification of technology acquisition scenarios in order to record, analyse, and report on the entirety of individual assessments, made by different actors and stakeholders involved. The focus of such a system is to guide the assessment process and improve the reflexivity of information, opinions, and expertise among the contributors and decision-makers in the assessment of technology impact. This is achieved by making salient the issues which have been assessed (and also those which have been ignored); whether certain actors have been left out of the process and should be included; where there is agreement or conflict between actors; and whether the collective assessments made are balanced in terms of the different interests and responsibilities of all actors involved. This is a novel approach and in stark contrast to most existing decision support systems which focus on computing key performance indicators to suggest particular solutions which embody the best trade-off between assessment criteria, but which may not necessarily present the best solution to choose in terms of other types of impact.

4.1 Introduction

Large-scale infrastructure projects in the field of mass transportation usually involve the deployment of a range of technological solutions in order to ensure compliance with existing policies and regulations on the national and transnational level,

R.R. Grau (✉)
Faculty of Science, Engineering and Computing, Kingston University London,
Kingston-Upon-Thames, UK
e-mail: r.r.grau@kingston.ac.uk

S. Gutwirth et al. (eds.), *Reforming European Data Protection Law*,
Law, Governance and Technology Series 20, DOI 10.1007/978-94-017-9385-8_4

especially those concerning security.[1] On a smaller scale, there are also projects that develop new technological solutions intended to solve existing security problems. In the recent past, there have been examples of such projects getting into trouble, and the mass media reported outcomes to range from severe delays in project delivery and the accumulation of substantial extra cost,[2,3] to possibly complete failure of the entire project.[4] While hindsight is always easier than foresight, it appears that some of these problems may be preventable in the future by facilitating technology impact assessments (TIA) in a way that involves more relevant actors and stakeholders, and that improves mutual communication and exchange of information among actors before any substantial financial commitments are being made.

Conducting comprehensive impact assessments of security technologies is a complex problem because different assessment perspectives and related domains of knowledge need to be taken into account (Fig. 4.1). These are associated to the travel- and security processes which are inherent to mass transportation facilities; and an associated range of legislative, cultural, economic, technical, ethical and societal impacts. Further, multiple tasks need to be performed and regulations complied with in planning, implementation, and testing; and allowances made for possible problems and changes that may come about in the course of a project. Finally, these aspects are embedded within a complex network of different actors and stakeholders, coming from various international organisations, carrying specific interests, responsibilities, and competences.

This chapter describes the features and conceptual underpinnings of a web-based software prototype which was created in the course of the SIAM FP7 project.[5] The term *assessment support system* was coined to characterise this system and distinguish it from common decision support systems[6] which use different methods to quantify a limited set of assessment criteria in order to try and determine a particular solution that best fits a purpose in comparison to others.

[1] E.g., European Regulation on common rules in the field of civil aviation security, EC 300/2008.

[2] "Cost Explosion: Price Tag for New Berlin Airport Keeps Rising", accessed March 5, 2014, http://www.spiegel.de/international/germany/5-billion-euros-costs-increase-again-for-berlin-brandenburg-airport-a-928989.html.

[3] "The curious case of Berlin's Brandenburg Airport: Will it ever open?", accessed March 5, 2014, http://www.newstatesman.com/business/2013/09/curious-case-berlins-brandenburg-airport.

[4] "German defense minister to face grilling over Euro Hawk debacle", accessed March 5, 2014, http://www.dw.de/german-defense-minister-to-face-grilling-over-euro-hawk-debacle/a-16964646.

[5] European Commission – CORDIS – Projects – SIAM, accessed March 4, 2014, http://cordis.europa.eu/projects/rcn/97990_en.html.

[6] George Marakas, *Decision support systems in the twenty-first century*, (Upper Saddle River, N.J., Prentice Hall, 1999).

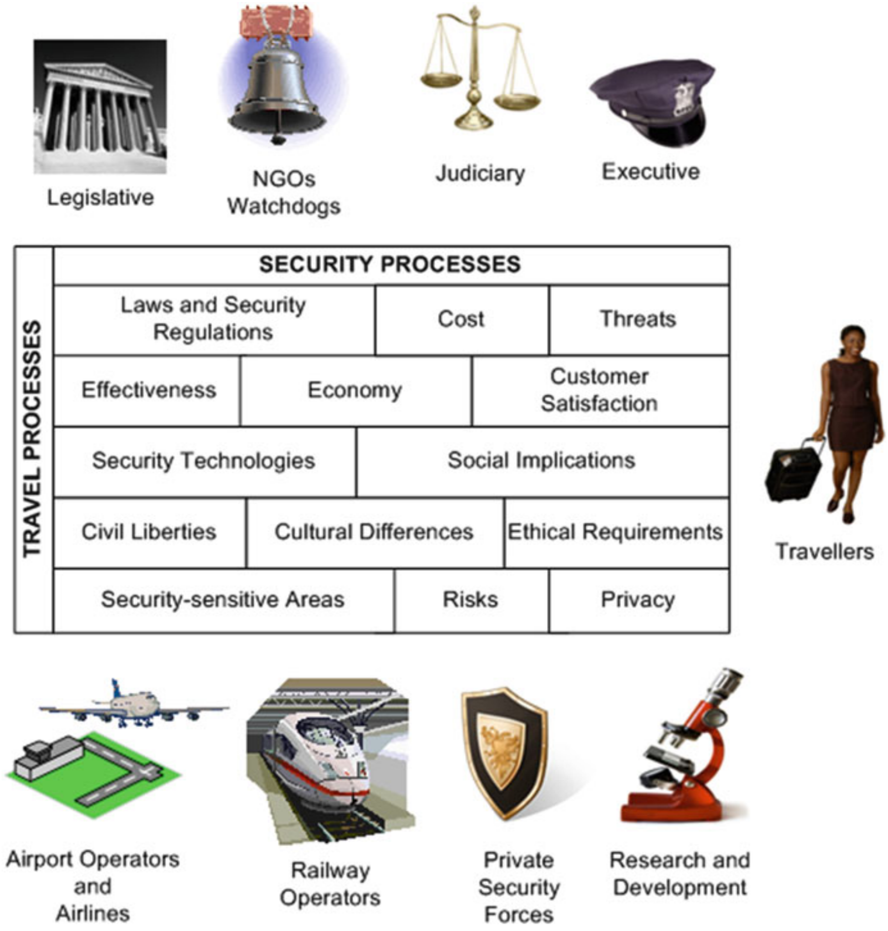


Fig. 4.1 A map of issues and actors in TIA in mass transportation (Figure translated, originally from: Hempel, Leon et al., "SIAM – Security Impact Assessment Measures. Ein System zur Unterstützung von Security Technology Assessments an Flughäfen und im öffentlichen Nahverkehr", Oranienburger Schriften, (Fachhochschule der Polizei des Landes Brandenburg. 2011))

Such systems would fall short in light of the complexity associated with more comprehensive technology impact assessments, where human reflection and judgment are generally considered to achieve better results. The aims of an assessment support system are to collect and structure the information elicited from different actors, and provide effective representations that help human assessors to navigate and deal with the vast space of assessment issues more easily. The system presented here makes use of an extensive catalogue of assessment questions that take different perspectives on the technological solution at hand, and elicits information about a planned technology acquisition, as well as expertise and opinions from the actors involved in the assessment. This information is then processed and compiled in a structured assessment report to give insight into how different actors have evaluated various aspects of a technology and its impact, to identify areas of agreement or conflict, and give guidance on aspects where the assessment process could be improved.

In essence, an assessment support system is more concerned with the process rather than the result. That means the particular measures employed to provide guidance and decision-support do not directly point towards a particular technological solution that seems to be more favourable than another, based on performance measures, for example. In contrast, an assessment support system uses a range of semantic metadata of the issues addressed, and of the actors who address them, in order to also indicate higher-level properties of the assessment process itself. For example, this is useful to find out whether the assessment of certain topics was balanced, in terms of a sufficient number of different relevant actors having contributed their view; or, to point out whether certain actors are currently missing and should be included in the assessment. In this general way, an *assessment support system* is meant to enhance, rather than replace, traditional decision support approaches. The focus here is to guide the assessment process and improve the reflexivity of information, opinions, and expertise among the contributors and decision-makers as they engage in technology impact assessment.

In the next section, the application context for which an assessment support system has been developed will be described, followed by details on some related knowledge which has informed the design of the software system. In particular, details will be provided on the kinds of users which were considered for the software, how activities were mapped to specific user interactions, and a general overview of the system's architecture. In Sect. 4.3, some of the conceptual underpinnings of the system will be discussed. Finally, the main features of the software will be presented in Sect. 4.4, followed by some details on the evaluation procedures in Sect. 4.5, and a closing summary (Sect. 4.6).

4.2 Application Context and Mapping

This part provides an overview of the assessment process supported, details on how this process was mapped to a general use case to be implemented in software tools, and a description of the overall architecture envisioned for the computational assessment support system.

4.2.1 Background

The application context for the software is situated in the field of security technology acquisition. In particular, the related decision-making processes in mass transportation sites have been taken as an exemplar for devising an abstract,

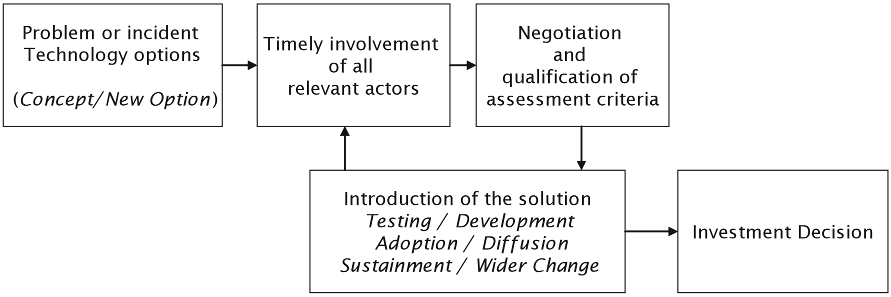

Problem or incident
Technology options
(*Concept/New Option*)
Timely involvement of all relevant actors
Negotiation and qualification of assessment criteria
Introduction of the solution
Testing / Development
Adoption / Diffusion
Sustainment / Wider Change
Investment Decision

Fig. 4.2 General phases of the idealised SIAM assessment process (From: Graeme Jones and Ronald Grau, "The SIAM Assessment Support System: Initial Application and Database Specification", SIAM deliverable D11.1, (European Commission, 2012), 6)

idealised assessment process which should be supported by a software system (Fig. 4.2). This development was informed by a series of case studies conducted with industrial partners from the mass transportation domain, such as airport and railway operators.[7] The case studies were based on the idea of reconstructing the innovation journeys[8] of previous technology acquisitions at the respective sites, and concerned the elicitation of related information such as the relevant actors involved, assessment criteria applied, and the structure of the overall decision-making process.

In this context, an assessment is made in the context of evaluating technology options for solving new or existing security problems. Figure 4.2 shows the basic activities underlying this process. At the beginning of the assessment process is a scenario formulation phase, where the security need is explained, and a technological solution suggested. This information is usually available as result of a locally conducted threat assessment and constitutes the beginning of the "Concept/New Option" phase of the technology acquisition process. In this phase, a problem has been identified and technological solutions are being considered to address the problem.

Different actors get involved in a subsequent evaluation process which may have different roles, depending on the stakeholders they represent, and their associated interests, needs, motivations, and responsibilities. The different actors engage in the definition and negotiation of the assessment criteria that are deemed important to consider before a decision is made about whether an investment into some technology option should go forward. After the first phase, part of the process is repeated to address further phases of the technology acquisition process, such as "Testing/Development", for instance, which may involve other actors and related assessment criteria. This idealised process assumes that after the technological

[7] Leon Hempel et al., "Innovation Journey Report", SIAM deliverable D2.4, (European Commission, 2011).

[8] Andrew van de Ven et al., *The Innovation Journey,* (New York: Oxford University Press, 1999).

solution has been further assessed in the context of development, implementation, testing, diffusion, sustainment, and wider change, a well-informed decision can be made.[9] Since every phase will invokes different sets of actors and assessment issues, the first one ("Concept New Option") was chosen as an exemplar for demonstrating the capabilities of an assessment support system in the course of the SIAM project.[10]

4.2.2 General Use Case

The development of a software system usually involves the design of one or more use cases mapping a problem-related workflow to purposeful human interactions with a user interface.

At its core, the assessment process illustrated in Fig. 4.2 has been realised through a mechanism involving three major steps (Fig. 4.3):

1. In the *assessment configuration* step, a specific *assessment case* is created which has all relevant information about a given scenario and the suggested solutions, a technology proposal for addressing the problem, and a first set of actors which are to be involved in the assessment case (which can later be extended).
2. *Assessment questions* are posed to the actors about the particular problem scenario which is to be assessed, covering a wide range of topics concerning organisational, economic, technological, legal, societal, as well as trust- and security-related issues. The questions are aimed towards acquiring information from different perspectives, targeted at particular actors, and differentiated by the particular attributes of the technological solution proposed. In other words, the configuration of the assessment case determines the kinds and number of particular questions asked, such that those which are not relevant for the current

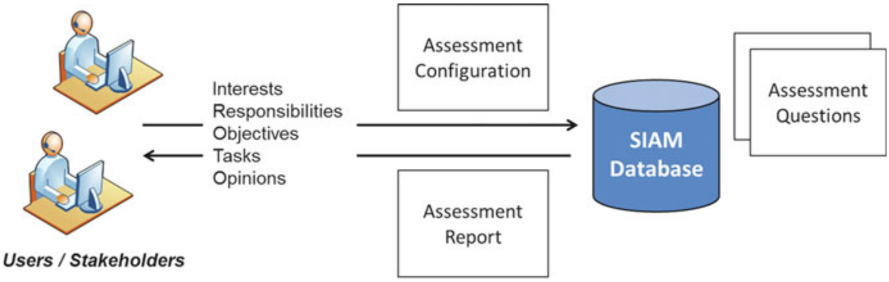


Fig. 4.3 General use case mapping of the SIAM assessment support process (From: Ronald Grau and Graeme Jones, "The SIAM Assessment Support Toolkit: A Software System for the Support of Technology Impact Assessments", SIAM deliverable D11.2, (European Commission, 2014), 10)

[9] For the definitions of the phases, please refer to Hempel et al., "Innovation Journey Report", 7–8.

[10] European Commission – CORDIS – Projects – SIAM.

case can be hidden. Semantic data is used to target questions more effectively to the different actors, and questions can be interconnected and have mutual conditions in place which control their presentation. The answers given by the various actors are eventually stored in a database and associated with the current case.

3. *Assessment reports* can be compiled from the information gathered for a case which summarise the contributions made by the actors and show an analysis of the answers given based on the defined assessment perspectives, tasks, and subjects, in order to provide further guidance on how the assessment process can be improved to achieve a more comprehensive and reflective evaluation of the proposed solution.

4.2.3 Actor Roles and User Functions

For the design of a software system, it is important to determine the kinds of users which will interact with it before any useful features can be implemented. Aside from scientific researchers who are free to take any particular stance in using the system, two distinct actor groups and some of their roles, responsibilities and interests were initially identified:

Policy Setters

- ***Stakeholders:***
  Transport and Civil Aviation Authorities, Watchdogs, Non-Government Organisations
- ***Roles:***
  Establishers and enforcers of security standards and regulations, Supervision of facility managers, Safeguards of security and safety, Creators of subjective security, Safeguards of freedom and fundamental rights.
- ***Responsibilities:***
  Compliance with other legalistic requirements, realisation of state policies, Increasing homeland security, Maintaining passenger rights, Harmonisation of legal frameworks, Funding of research, Identification of infringements, Demanding or creating counter infringement measures and –technologies.
- ***Interests:***
  Understanding threats, understanding security measures and -technologies, Advocating privacy and data protection, Understanding infringements, international recognition and acceptance.

Policy Implementers

- ***Stakeholders:***
  Facility managers, Facility personnel, Police and contracted security providers.
- ***Roles:***
  Investors, Implementers, Providers of retail space, Operators, Police forces.

- ***Responsibilities:***
  Operating a transport facility within a business context subject to the security requirements specified in security policies, Legal compliance.
- ***Interests:***
  Keeping up a secure state of the facility (prevent damage and disturbance of operations), Retail income maximisation, Security Investment optimisation, Minimising acceptance issues (including Convenience, Health and Infringement implications).
  Source: SIAM Initial Application and Database Specification[11]

In addition to a specification of professional roles for the participants in an assessment case which reflect certain interests and responsibilities of the related stakeholders, it was also recognised that the users of the system must perform different tasks, or functions, which are more closely related to what they do when using the software. Consequently, *user functions* were introduced as a means for distributing different organisational and contributory tasks in the assessment process (Table 4.1). These user functions go along with certain permissions and access rights to features of the software that are relevant for each user to fulfil their particular set of tasks. The functions are, in principle, independent of an actor's role.

Table 4.1 User functions in the SIAM AST

Function	Permissions
Assessment leader (Coordinator)	Can set up new assessment cases
	Can specify and invite other actors
	Can answer assessment questions
	Can edit and generate the overall assessment report
Assessment participant	Can access assessment cases (once invited)
	Can answer assessment questions according to their specified role
	Can create custom questions to be considered by other actors
	Can generate a summary report of their personal contributions
Information provider (External consultant)	Can access specific assessment cases (once invited)
	Can answer only those assessment questions which have been delegated by other actors
Observer (Auditor)	Can access specific existing assessment cases
	Cannot answer any questions
	Can inspect the assessment report

[11] Jones and Grau, "The SIAM Assessment Support System: Initial Application and Database Specification", 10–11.

For instance, any user of the software can create assessment cases, which assigns the function "Assessment Leader" to that particular user, limited to the case created. The same user could fulfil different functions in other assessment cases, acting as a participant, observer, or information provider.

4.2.4 System Architecture

In the assessment of security technologies, there is a need to adhere to established standards and utilise up-to-date information that can be retrieved from the public domain or from government authorities (e.g., legal texts, open standards, technical reports, crime statistics, threat assessments, research papers, etc.).[12] On the other hand, there is also a desire to keep certain information within the facility or institution where an assessment is made, such as the physical layout of security sensitive areas, the functionality of existing installations, or the contents of location-specific threat scenarios. Based on these considerations, the assessment support system was envisioned to make use of distributed data, with some information retrieved from the external sources, and further, privately held information about facility-specific models of threats, processes and technologies. This is not to say that local information cannot be shared: It is imaginable that an exchange of relevant standards, best practices, assessment criteria or -scenarios between organisations can in fact bring positive synergy effects and improve the speed and quality of technology acquisition processes overall. However, a separation of the data will leave the assessing facility or institution in control of what private data to share and with whom.

At the heart of the computational implementation is a browser-based application that implements the mapped SIAM assessment support process.[13] The application runs on a web server, and can be installed at different local sites. Private data is kept in a local database, and public assessment information retrieved over the Internet from other repositories, provided and maintained by public institutions or government authorities. Figure 4.4 shows how this architecture could look like should the system be chosen to be adopted and deployed at a comprehensive, possibly national or transnational scale.

Within the SIAM project, the aim was to create a prototype of such a system which illustrates the capabilities of the assessment support application. As the partnerships with policy setter organisations which are required for implementing the above approach are clearly not existent in this phase of development, the architecture was simulated with a local demo database, which was used for storing all data. The prototype functionality comprises a modular software platform which

[12] E.g., see Kristof Verfaillie and Rosamunde van Brakel, "Assessing security threats in mass transportation sites", SIAM Deliverable 6.2, (European Commission, 2012).

[13] See Sect. 4.2.2.

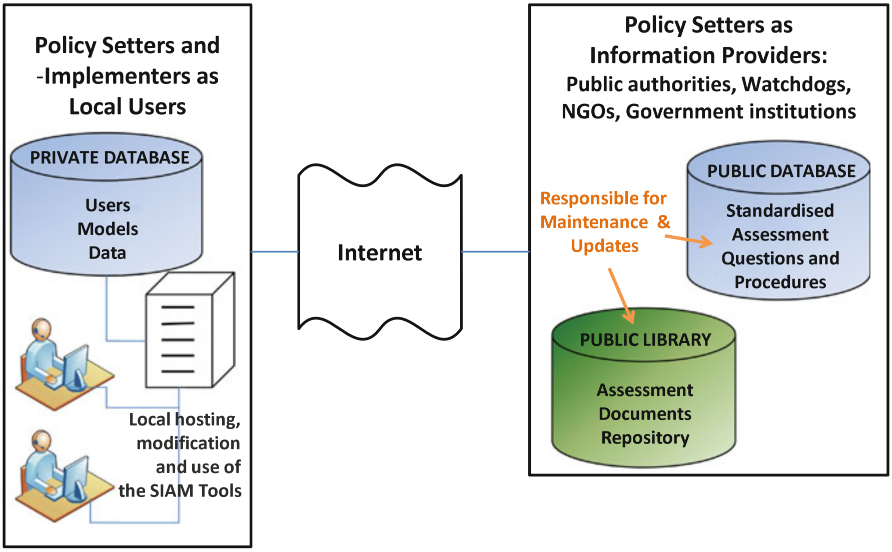

Policy Setters and -Implementers as Local Users
PRIVATE DATABASE
Users
Models
Data
Local hosting, modification and use of the SIAM Tools
Internet
Policy Setters as Information Providers:
Public authorities, Watchdogs, NGOs, Government institutions
Responsible for Maintenance & Updates
PUBLIC DATABASE
Standardised Assessment Questions and Procedures
PUBLIC LIBRARY
Assessment Documents Repository

Fig. 4.4 General architecture of the SIAM AST (From: Jones and Grau, "The SIAM Assessment Support System: Initial Application and Database Specification", 12)

has a technology impact assessment support application as core unit. A database stores various kinds of assessment information, such as that about the actors involved in the technology acquisition process, their particular roles, as well as the assessment criteria and questions that need to be considered. Within the assessment support application, these questions are then posed to users of the system in a structured fashion; information is collected from the users; and reports are generated based on the questions which were asked and the answers that were received.

4.3 Conceptual Developments

Software development is substantially informed by requirements engineering activities where subject experts provide the necessary information and knowledge required for the design of suitable software components.[14] As the SIAM project aimed to include information related to several factual and process-based concepts, such as different kinds of *technology*, *security measures*, *threats*, and various *impacts*, a conceptual basis needed to be developed for inter-relating the relevant information. This presented a tremendous challenge, as many of those concepts form a complex domain of their own. The task of a software architect is to gain a

[14] For some common approaches, see I. Sommerville, Software Engineering, 7th ed. (Harlow, UK: Addison Wesley, 2006).

sufficient conceptual understanding to be able to design the required software functionality. For this purpose, the conceptual models employed do not need to represent all domains in their full complexity and detail; they merely need to be adequate for the purpose such that they facilitate the design of data structures and functions to implement a specified use case in a software program. The conceptual models also need to be sufficiently general in order to enable understanding and communication about the assessment issues between different kinds of users of the software, considering these may have different areas and levels of expertise. As a result, somewhat simplified structures are often adequate to represent and interconnect information about processes and impacts at an abstract conceptual level, whereas the complexity of individual assessment issues can be expressed through carefully designed assessment questions. There have been previous efforts to structure and model the entities and relations that exist in the security domain.[15,16] These provided useful inputs for modelling but were found to be of limited use as an off-the-shelf conceptualisation, considering the ambitious development goals of SIAM.

This section presents some of the conceptual ideas and models developed as a result of the requirements engineering activities mentioned above. These were conducted as knowledge elicitation and modelling exercises performed in workshops, surveys, and direct requests for information targeted at the content-providers available in the project, which included sociologists, criminologists, lawyers, engineers, and technologists from various international organisations. The conceptual ideas reflect the conceptual mapping of any knowledge retrieved into structured representations that can be implemented into computer programs. These models might not present a universal solution for all impact assessments and be quite specific to the current security technology application context, and the requirements of the software. However, they may be useful for other computer scientists that work in related areas or to inform future extensions of this work. Those readers who are mainly interested in the description of the implemented features can skip this part and go directly to Sect. 4.4.

4.3.1 Security Measures and Technologies

One of the core concepts of the system relates to the so-called *Security Measures and Technologies* (SMT) which are being assessed. In the most general sense, *technology* refers to the procedures and technical artefacts which have been designed for a particular purpose. In our model, technology is thus present in both an *activity* and a *tool*. SIAM's conceptualisation of SMT has been based on a process-based

[15] E.g., "A Global Approach for European Civil Aviation Security", White paper, Version 1.0, (EOS Civil Aviation Security Working Group 2009).

[16] E.g., Annex 17 to the Convention on International Civil Aviation – Security – Safeguarding International Civil Aviation against acts of unlawful interference, Ninth edition, (International Civil Aviation Organization, 2011).

view of the security domain which identifies the nature of security policies as the defining element for security measures, which are purposeful activities in the first place. The model then differentiates the *actions* for achieving the purpose of a policy from their implementation aspects, i.e. the *actors* and/or *technology* involved in executing the actions.

In essence, the underlying idea of this model is that every *Security Process* comprises one or more *Security Measures*, which are further described by three components: *Actors, Activities, and Tools*. Based on the specification of some security need or purpose (*Security Policy*), *Security Processes* can be represented as *Security Policies* that are implemented by the components of *Security Measures* (Fig. 4.5). This approach considers that *technology* refers to more than just the naïve perception of technical devices. A big advantage of describing security measures and technologies at this level of granularity is that relations to other concepts like threat, infringement, or trust can be established that are sufficiently meaningful to aid decision-makers in their evaluation of an SMT. Extension of this model were created to determine the relations, where *Threats* can be described in a similar fashion and connected to existing models of SMT. For instance, consider a handgun is an object that could be defined as the *tool* of a threat, and a statement can then be made whether this tool can be detected by a component of a particular security measure.[17]

Real-world impact assessments do not usually address single technologies rather than complex technology stacks embedded within solutions, where every individual

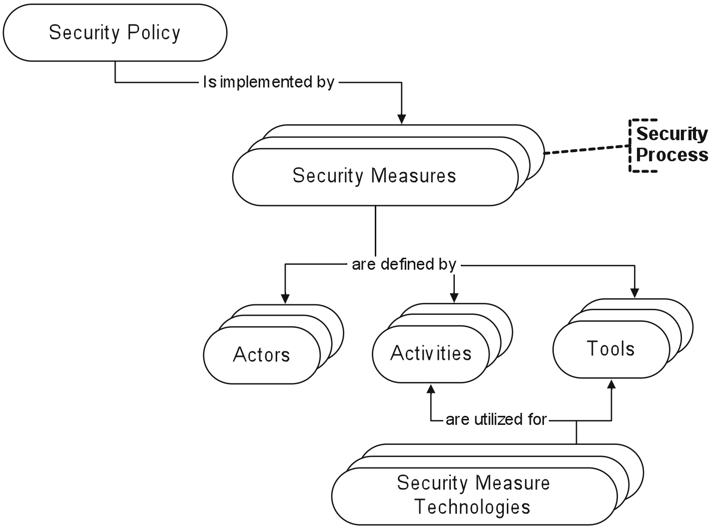


Fig. 4.5 A process-based model of SMT (From: Graeme Jones and Ronald Grau, "A Typology of Security Measure Technologies and Counter Infringement Technologies", SIAM deliverable D2.3, (European Commission, 2012), 6)

[17] See also Sect. 4.3.3.

part may have a distinct impact on various issues, depending on what it is used for. For example, a person- or luggage scanner device actually combines a number of different technologies for imaging, analysis, reporting, etc., in order to offer a technological solution to a problem, and in compliance to the policies outlined in a security plan. With respect to infringement and the development of counter-infringement measures and technologies, the resolution adopted by this knowledge representation allows pinpointing quite clearly what exact part of a security solution presents a problem, acknowledging that it is actually part of a wider security process involving human operators and their specific activities, as well as architectural elements and economic constraints. For example, a body scanner is a complex technological solution, where the radiation emitted by some technical part (*tool*) may be the origin of health problems and thus, possible infringements of the bodily integrity of the scrutinised. Further, the officer inspecting the images delivered by the solution may be an *actor* carrying out an *activity* responsible for privacy issues. This list of examples could be continued easily.[18]

The range of security measure technologies that need to be grouped within this typology is enormous. To provide a practical limit to this range yet enable future extension, the following scoping has been adopted (Fig. 4.6). The *Protection* domain can be partitioned into two broad categories: *Safety* and *Security*. The *Safety* category includes accidental or environmental sources of threat such as fire, severe weather, flooding and major accidents.

The S*ecurity* category addresses threats that mainly arise from deliberate human action. The *Security* category addresses threats to both the physical and the informational realm. The SIAM project focused on security measures and technologies that address the *People and Physical Infrastructure* category which is a sensible constraint as many of the assessed impacts (e.g., infringement of rights, norms and other liberties, or socio-technical normativity, etc.) do not apply to the virtual realm

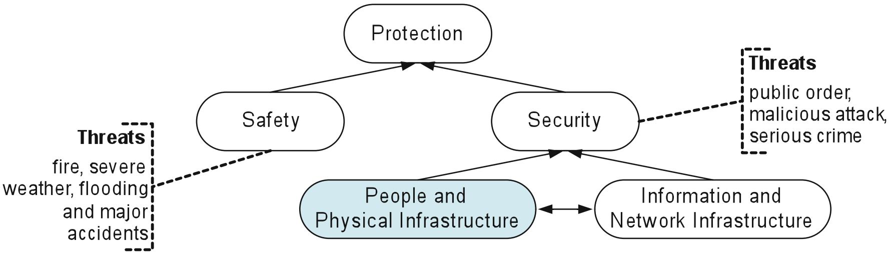


Fig. 4.6 A protection typology (From: Jones and Grau, "A Typology of Security Measure Technologies and Counter Infringement Technologies", 7, 5)

[18] Cf. Jones and Grau, "A Typology of Security Measure Technologies and Counter Infringement Technologies", 7, 23.

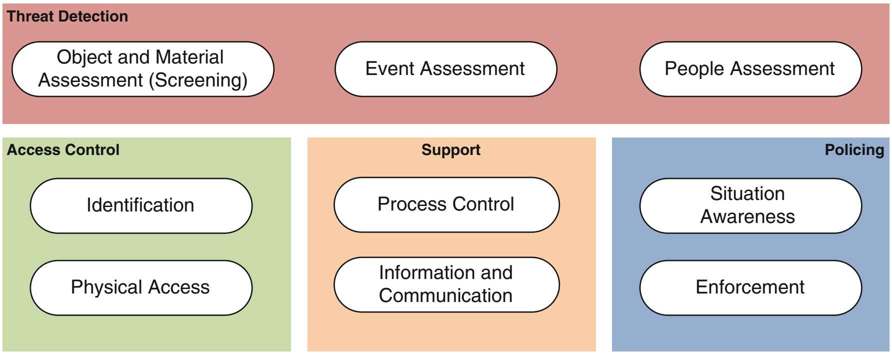


Fig. 4.7 The SIAM SMT typology (Figure and subsequent descriptions: Jones and Grau, "A Typology of Security Measure Technologies and Counter Infringement Technologies", 8)

and thus need to be examined at a level where information technology and people intersect.[19]

Given the conceptualisation and the scoping constraints outlined above, Security Measure Technologies (SMT) can be broadly partitioned into nine subclasses embedded within four groups, as shown in Fig. 4.7, and further detailed in the following sub-sections. The grouping of the SMTs corresponds to main directives of a security regime, some of which were taken from current security plans.[20] Further, the typology accommodates measures that are commonly classified as either *preventive* or *corrective measures*, as well as measures used for *establishing* and *protecting* the *security status* of objects or people within a facility.

In the following, the individual groups, and the types embedded within the groups will be described in more detail.

4.3.1.1 SMT Typology

Threat Detection

Threat Detection SMTs are used in security measures designed to detect potential threats by some signature of the attack. Both *Threat* and *Security Measure* can be modelled as a *Process* carried out by *Actors* using *Tools* to carry out an *Action* or *Activity*. Threat detection, therefore, can focus on the actors, the actions related to an event or the tools used.

[19] Jones and Grau, "A Typology of Security Measure Technologies and Counter Infringement Technologies", 5.

[20] E.g., Regulation (EC) 300/2008.

- ***Object and Material Assessment SMTs*** are used within security measures to search and assess people, luggage, cargo and airport deliveries to identify possible dangerous or illegal objects and substances e.g. weapons, drugs, or explosive residue.
- ***Event Assessment SMTs*** attempt to identity an unfolding crime by, for example, using surveillance to detect *suspicious behaviour* or to spot *abandoned luggage*.
- ***People Assessment SMTs*** are used in measures designed to identify potential malefactors. This includes questioning strategies, profiling methodologies such as background checks of passengers, or asymmetric screening based on demographics.

Access Control

Segregation of different user groups and objects is a standard security mechanism for preventing access to security-sensitive areas, protecting the security integrity of individuals or objects which have passed the checks carried out during a security process. Maintaining the integrity of facility will also require establishing identity and the right to access, and ensure those without a right to access are excluded.

- ***Identification SMTs*** are used to identify people as part of security measures designed to establish access rights.
- ***Physical Access SMTs*** relate to the broad category of physical barrier and access technologies such as turnstiles, perimeter fencing, and automated car park barriers.

Support

Some technologies are used to enable and support security processes yet do not present security activities in their own right. This general category refers to technologies for controlling the general function and performance of security measures and the information and communication systems and processes that underpin any security system.

- ***Process Control SMTs*** capture the range of technologies that configure the security process including the control of passenger flow, and the randomised or intentional selection of security measures applied to individual passengers.
- ***Information and Communication SMTs*** capture the computing and communication technologies used for a variety of different security measures within any security regime, such as those which can be found in devices and algorithms for information processing, as well as data transfer and storage.

Policing

In general terms, the SMT category *Policing* refers to those technologies used to maintain an understanding of what is happening within a controlled area and to those technologies which enforce compliance and contain imminent threat.

- ***Situation Awareness SMTs*** includes the use of surveillance camera systems to monitor an environment and liaise with staff on the ground, and the use of asset management solutions such as Radio-frequency identification (RFID) tags and readers to track luggage and passenger movements or automated number plate recognition technology to identify vehicles.
- ***Enforcement SMTs*** are technologies used in security measures that respond to some process deviation or detected threat, such as those ensuring passenger every piece of hand luggage is screened or those dealing with a detected weapon.

4.3.2 Assessment Question Pool

Including a wide range of impacts in the assessment of technologies requires a large number of assessment questions to be addressed. In terms of its technical role in the software, the *Assessment Question Pool* presents a complex set of data structures and control mechanisms, required to manage the authoring and storage, as well as the targeted presentation (i.e., relevance) of assessment questions.

In relation to a specific assessment case, the term refers to the total number of assessment questions relevant for the technology assessed in this particular case. For instance, the assessment of an *Identification SMT* could invoke a somewhat different set of questions than the assessment of an *Event Assessment SMT*. Individual users participating in a case are allocated a subset of assessment questions from this pool, based on their particular actor-role specification. In other words, an actor in the role *Lawyer* might see slightly different questions than an *SMT Investor*. The decision on which relevance criteria apply is made during the authoring of an assessment question. The current assessment support toolkit comes with a demo question pool created by the partners of the SIAM project who made these relevance decisions based on their professional expertise.

4.3.2.1 Brief Overview on Concepts and Structure

Each assessment question is defined within a hierarchy of *topics* and subordinate *aspects* which provide a more specific context for this question. For example, assessment questions about freedom infringement might address the topic “Bodily Integrity”, and its dependent aspect “Intrusiveness”. The SIAM demo question pool currently has 45 topics, and 180 dependent aspects distributed between these topics. An assessment question has various further attributes and data elements, which are organised through two major concepts: *screens* and *screen groups*.

A *screen* contains textual information which a user would see when presented with a *single question*, such as a question heading, an introductory text, and the actual question text. A screen also involves configurational and relational information which includes the type of answer expected, the particular *assessment perspective* (a semantic attribute) addressed by the question, an associated *assessment task* (a second semantic attribute), and supplementary resources that should be presented when the screen is shown.[21] Each screen has a specification of the SMTs to which it applies and the actors to which it should be presented.

A *screen group* is a container for one or more screens, in other words, a grouping element for questions. The questions within a particular screen group share the same context definition (topic and aspect). The purpose of screen groups is to organise those questions that are closely related to each other and allow additional constraints to be defined for their presentation. For example, all screens in a screen group can be ordered to be presented in a particular sequence. This allows for the formulation of several questions to explore and assess the same issue, like when going from a very general question to more specific ones.

4.3.2.2 Controlling Relevance with Conditions

Screens that reside within the same screen group can have additional conditions placed upon them which control their presentation, based on answers given to specific previous questions in the same group. For instance, there could be an initial Yes/No question, followed by another which elicits more details. If both questions are in the same group, a condition can be specified for the second question to be shown only if the answer to the first question was "Yes". When screen groups are set up to contain conditional questions, this provides for a very effective way of controlling the gathering of assessment information based on user responses. When selecting a question for presentation to some user, the SIAM AST will first select all available screen groups based on their context definition, and then further evaluate whether any questions that reside within these groups should be shown to the current user and in the current case. The question pool delivered by the SIAM project contains 586 assessment questions in total, of which 269 are non-conditional questions. The majority of questions concern legal and societal issues from the perspective of *Freedom Infringement* and *Trust*.

4.3.3 Further Core Ideas and Models

The conceptual underpinnings of the support system include other models and ideas which present logical extensions of the basic security domain model described in

[21] For the specific *perspective* and *task* definitions adopted by SIAM, see Grau and Jones, "The SIAM Assessment Support Toolkit: A Software System for the Support of Technology Impact Assessments", 7–9.

Sect. 4.3.1 and the SMT typology derived from it. A detailed description of these could not be included in this chapter but they shall be mentioned briefly, including references for further details. Some of the additional conceptual developments underpinning the assessment support system include:

- A model involving *Infringement* concepts and mechanisms, which generally describes infringement as damage in relation to different kinds of individual assets, distinguishing codified and subjectively perceived infringement, as well as various types of actual, potential, direct, indirect, immediate, or delayed damage.[22]
- Based on the above, a process-oriented conceptualisation of *Counter infringement measures and technologies*, and a description of the relation to *Security measures and technologies*.[23]
- Based on the above, a derived *Typology of counter infringement measures and technologies*, grouped according to common properties characterising a capability to reduce the scope and intrusiveness of an infringement.[24]
- Based on the above, ideas for devising *Infringement profiles* as attributes of SMTs, based on the identified kinds of infringement identified with particular SMTs.[25]
- A process-oriented model of *Threat* and a description of how this intersects with security processes and SMTs.[26]
- Based on the above, *Threat signatures* as attributes characterising different threats, and the implications for identifying the capabilities of different SMTs to detect or mitigate such threats.[27]
- Based on the above, a basic model of crime (which defines crime as a subset of threat) and a description of how this could be related to security measures and technologies.[28]
- Based on the above and the similar conceptualisation used in the context of threats, *crime signatures* to characterise different kinds of crime, and the implications for identifying the capabilities of different SMTs to detect or mitigate those crimes.[29]

[22] Jones and Grau, "A Typology of Security Measure Technologies and Counter Infringement Technologies", 19–23.

[23] Ibid., 23–24.

[24] Ibid., 26–27.

[25] Ibid., 24–26.

[26] Graeme Jones and Ronald Grau, "Updating the SIAM Application Specification from WP6", SIAM deliverable D6.4, (European Commission, 2012), 7–8.

[27] Ibid., 9–12.

[28] Graeme Jones and Ronald Grau, "Updating the SIAM Application Requirements: Crime-modelling and ASS tool development activities", SIAM deliverable D7.3, (European Commission, 2013), 5–6.

[29] Ibid., 6–7.

These developments were largely based on knowledge engineering activities which were carried out in collaboration with the partners of the SIAM project and were utilised in the design of the software to different extent, either informing the development of data structures to implement certain features (for instance, the gathering of threat assessment information during assessment case configuration) or simply to enable the future extension of the current prototype with related features.

4.4 Assessment Support Tools

Different tools have been developed and assembled to form the *SIAM Assessment Support Toolkit* (SIAM AST). Due to the different nature of the tasks that users of the toolkit can perform, the software platform has been structured into a user- and an administration level. The user level interface is intended to provide access to the functionality that is directly related to assessment support tasks, like creating assessment cases, inviting actors, performing assessments, and creating reports. The administrative level has facilities for creating and editing data that are necessary to run the application, to manage users, and advanced options for modifying the data at the system core. It was implemented to also allow anyone to reuse the structure and mechanics of the assessment support system in fields other than mass transportation in the future. A detailed technical description of the system, its administration features, as well as instructions for installation can be found in the system specification.[30] The focus of this section is to give a brief overview of some of the user level functionality.[31]

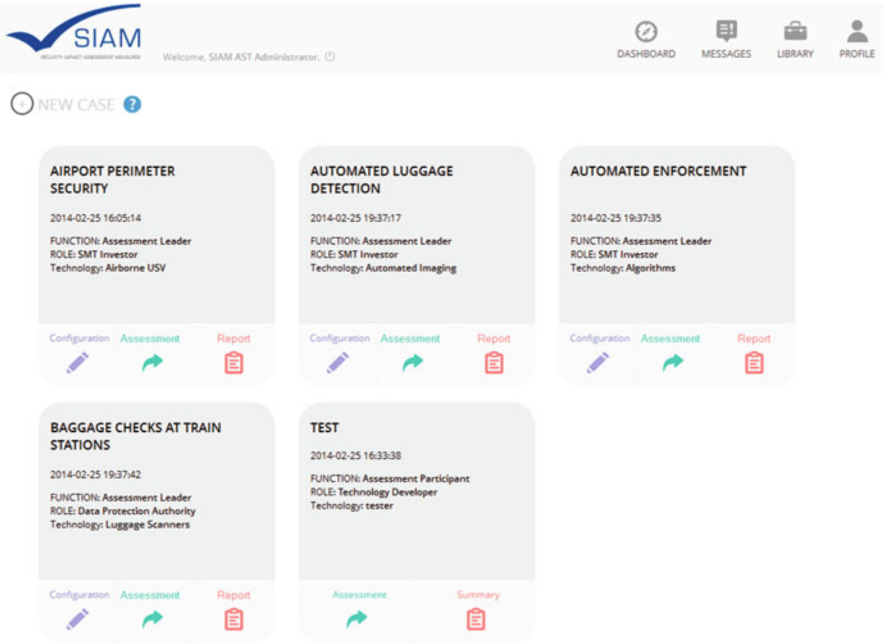
4.4.1 General Features

The toolkit is a web-based application and supports multiple users to jointly work together at the same time. Hence, it is possible to involve a substantial number of actors or stakeholders in an assessment case. Each actor is provided with their own user account to log on to the system. Actors can be assigned to different assessment cases, and may perform different functions and tasks in these cases.[32]

[30] Grau and Jones, "The SIAM Assessment Support Toolkit: A Software System for the Support of Technology Impact Assessments".

[31] Describing the entire range of interactive functionality verbally would require much more space than is available here. Note that the SIAM AST is free software and available for download at http://staffnet.kingston.ac.uk/siam/download/.

[32] Described in Sect. 4.2.2.



Welcome, SIAM AST Administrator.

AIRPORT PERIMETER SECURITY
2014-02-25 16:05:14
FUNCTION: Assessment Leader
ROLE: SMT Investor
Technology: Airborne USV

AUTOMATED LUGGAGE DETECTION
2014-02-25 19:37:17
FUNCTION: Assessment Leader
ROLE: SMT Investor
Technology: Automated Imaging

AUTOMATED ENFORCEMENT
2014-02-25 19:37:35
FUNCTION: Assessment Leader
ROLE: SMT Investor
Technology: Algorithms

BAGGAGE CHECKS AT TRAIN STATIONS
2014-02-25 19:37:42
FUNCTION: Assessment Leader
ROLE: Data Protection Authority
Technology: Luggage Scanners

TEST
2014-02-25 16:33:38
FUNCTION: Assessment Participant
ROLE: Technology Developer
Technology: tester

Fig. 4.8 SIAM AST – dashboard, showing some example assessment cases

4.4.1.1 Dashboard and Main Menu

The dashboard (Fig. 4.8) is the central information and control page for an individual user of the toolkit. Users can create and configure new assessment cases, or participate in other cases to which they have been invited to contribute.

For each assessment case, there are three main actions corresponding to the main phases of the assessment support process. As the respective function of the current user can be different for each assessment case, this will determine which of those actions are available:

– Configuration: Finish or edit the basic setup of a case (Configuration phase)[33]
– Assessment: Start or continue the assessment (Information gathering phase)[34]
– Report: Generate a personal summary of contributions, or start the assessment report editor tool (Analysis and reporting phase)[35]

[33] See Sect. 4.4.2 for details.

[34] See Sect. 4.4.3 for details.

[35] See Sect. 4.4.4 for details.

In the main menu (Fig. 4.8, top-right), there is a range of graphical buttons, shown persistently across all different tools in the software kit, at the top of the application window. From left to right, the main menu buttons allow

- Navigating from any other active screen during assessment back to the *Dashboard*.
- Accessing the *Internal Messaging System* (see section below).
- Accessing the *SIAM Library*, a repository which contains all documents and web resources uploaded or specified during question authoring, such as conceptual papers, assessment methodologies, or legal texts, for example.
- Editing the user profile for modifying user information, e.g. changing the current login password.

4.4.1.2 Communication and Workflow Support

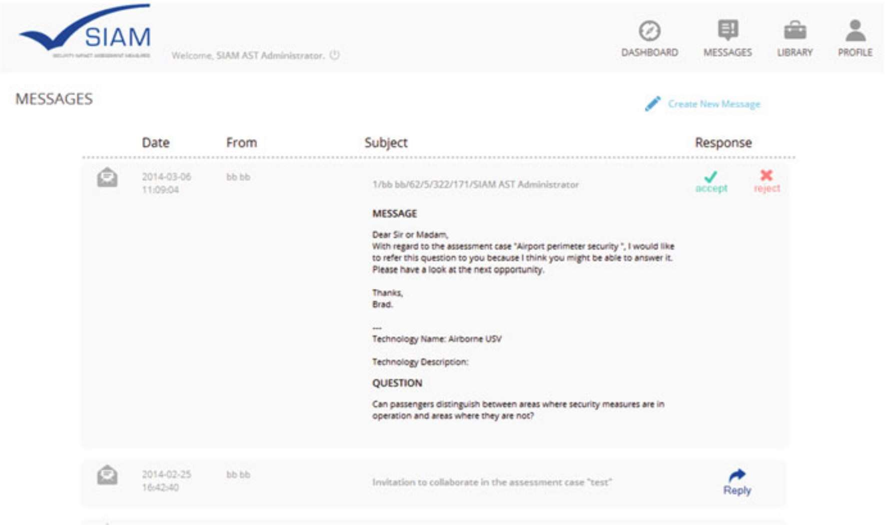
The SIAM AST includes an internal messaging system which is used to support assessment activities and the communication between actors in general. Apart from common messaging functions, where users can send each other text messages or questions, the tool is also integrated in other parts of the impact assessment workflow, such as

- Assessment leaders inviting other users to participate in an assessment case
- Users sending delegation requests for specific questions to other users
- The preparation and sending of notifications of delegation acceptance or rejection

Depending on the context in which a message is generated, the messaging system will offer to the users the necessary options to act. For instance, Fig. 4.9 is a screenshot of a user's messaging inbox, showing two messages. The upper, expanded, message is a delegation request from another actor which the current user can now decide to accept or reject. Upon selecting one of the options, a notification will be assembled and can be subsequently sent to the delegating actor. The lower, collapsed, message is an invitation to participate in an assessment case.

Main advantages of using an integrated communication platform for TIAs are that

- Specific communications can be customised to support the assessment workflow.
- Written communication between actors is contained within the assessment support system and not scattered across other channels (like e-mail), which provides for a better auditability of the assessment process.



Date	From	Subject	Response
2014-03-06 11:09:04	bb bb	1/bb bb/62/5/322/171/SIAM AST Administrator	✓ accept ✗ reject
2014-02-25 16:42:40	bb bb	Invitation to collaborate in the assessment case "test"	Reply

MESSAGE

Dear Sir or Madam,
With regard to the assessment case "Airport perimeter security ", I would like to refer this question to you because I think you might be able to answer it.
Please have a look at the next opportunity.

Thanks,
Brad.

Technology Name: Airborne USV

Technology Description:

QUESTION

Can passengers distinguish between areas where security measures are in operation and areas where they are not?

Fig. 4.9 SIAM AST – internal messaging system

4.4.2 *Assessment Case Setup*

The SIAM AST provides wizard-style input forms for setting up new assessment cases step-by-step. The configuration of an assessment case involves completing three different information sections across eight wizard steps:

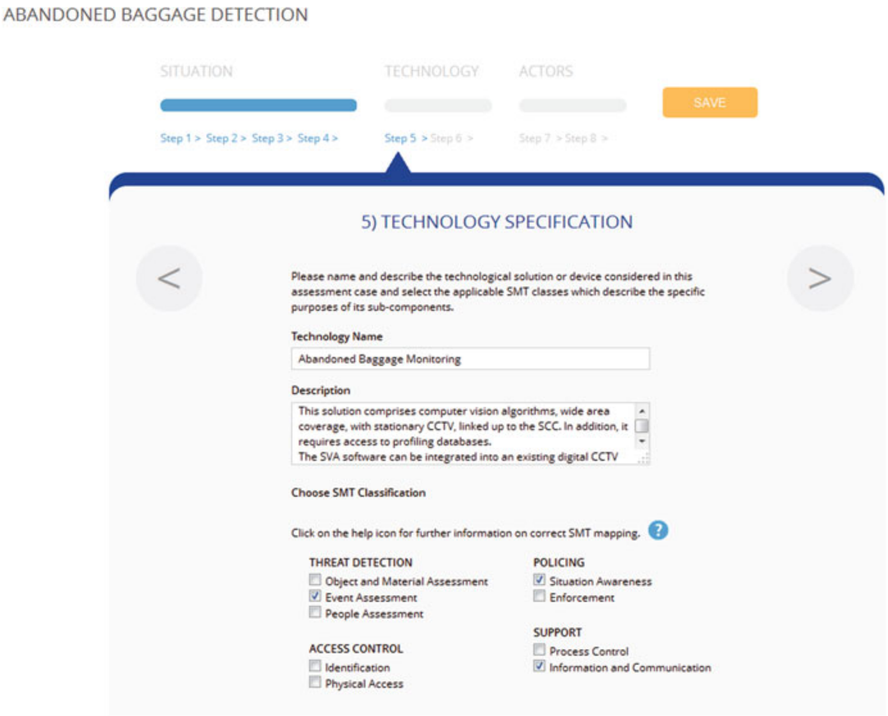
1. Information about the scenario or specific incident that triggered the need for performing an assessment and optionally, adding the results from an initial SIAM threat assessment workshop, if conducted.[36]
2. Information about the technological solution under consideration, the current technology acquisition phase, and the identified SMT types of the solution.[37]
3. Information about the assessment leader, as well as the other actors which are to be invited to contribute to or observe in the assessment case.

Figure 4.10 shows an example screenshot of the *Assessment Case Configuration Wizard*, in particular the fifth step, where the user is asked to make a specification of the technological solution which is being considered for assessment.

Selecting the correct SMT type(s) in this step is crucial for triggering the assessment questions that correspond to the technology, which are then shown to the participants during assessment, whereas those that are irrelevant will be hidden.

[36] For details on the methodology applied, see Yair Sharan et al., "Threat Scenarios Report", SIAM deliverable D6.3, (European Commission, 2012).

[37] See Sect. 4.3.1 for the SMT typology used.



5) TECHNOLOGY SPECIFICATION

Please name and describe the technological solution or device considered in this assessment case and select the applicable SMT classes which describe the specific purposes of its sub-components.

Technology Name

Abandoned Baggage Monitoring

Description

This solution comprises computer vision algorithms, wide area coverage, with stationary CCTV, linked up to the SCC. In addition, it requires access to profiling databases.
The SVA software can be integrated into an existing digital CCTV

Choose SMT Classification

Click on the help icon for further information on correct SMT mapping. ?

THREAT DETECTION
- □ Object and Material Assessment
- ☑ Event Assessment
- □ People Assessment

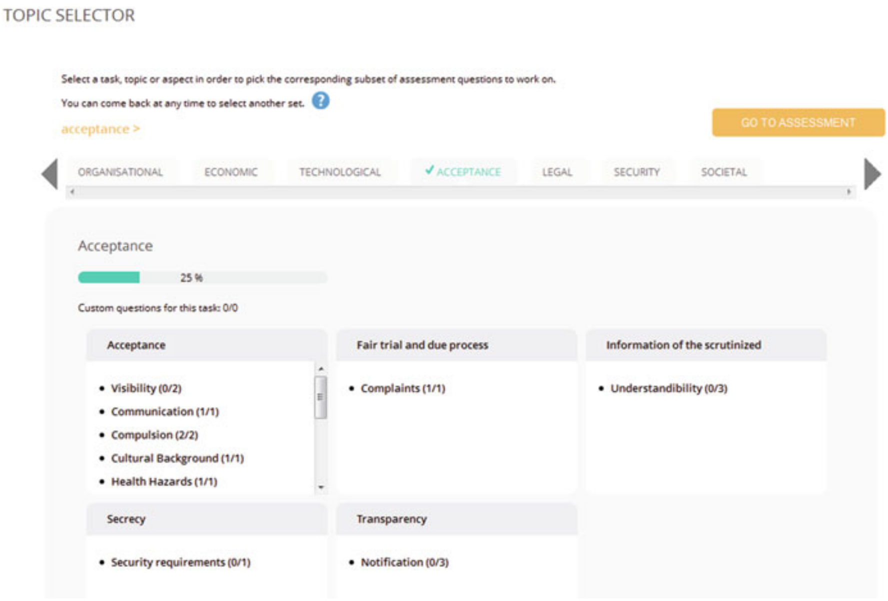
ACCESS CONTROL
- □ Identification
- □ Physical Access

POLICING
- ☑ Situation Awareness
- □ Enforcement

SUPPORT
- □ Process Control
- ☑ Information and Communication

Fig. 4.10 SIAM AST – example screenshot of the assessment case configuration wizard

This information will normally come as a result of a dedicated SIAM threat assessment workshop and involves decomposing the technology stack embedded within a solution in order to determine which general security policies the individual technologies in this stack implement. In the example below, the technology involves a camera system and computer algorithms to detect abandoned luggage at an airport. This corresponds to the SMT types *Event Assessment* and *Situation Awareness* (detecting incidents where luggage is considered abandoned, and tracking related objects), as well as *Information and Communication*, because video footage data is recorded, transmitted, analysed by algorithms, and possibly stored. For the sake of giving further examples, imaginable extensions of this technology could involve the camera system further examining the luggage to scan for dangerous substances (*Object and Material Assessment*) or taking of mug shots of any by-standing passengers to compare with passenger profiles, once an event is triggered (*People Assessment*). Selecting additional SMT types will generally increase the number of assessment questions that are posed to participants, however the selection shown to each contributing actor will also depend on their specific role. In the last step of the configuration process, actors are invited to participate in the case. Even after the assessment is in progress, an assessment leader can always go back to the configuration wizard and make changes, such as invite additional actors to the case.



TOPIC SELECTOR

Select a task, topic or aspect in order to pick the corresponding subset of assessment questions to work on.

You can come back at any time to select another set.

Acceptance

25 %

Custom questions for this task: 0/0

Acceptance
- Visibility (0/2)
- Communication (1/1)
- Compulsion (2/2)
- Cultural Background (1/1)
- Health Hazards (1/1)

Fair trial and due process
- Complaints (1/1)

Information of the scrutinized
- Understandibility (0/3)

Secrecy
- Security requirements (0/1)

Transparency
- Notification (0/3)

Fig. 4.11 SIAM AST – topic selector

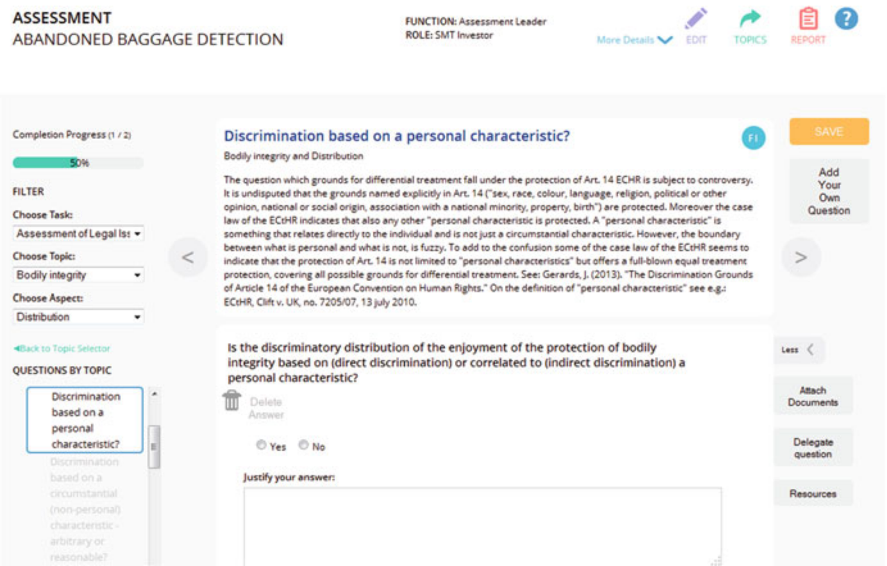
4.4.3 Information Gathering

This part of the toolkit concerns all activities related to actors answering an allocated set of assessment questions. After an assessment case has been set up, this case will appear on the dashboard of all invited users (e.g., see Fig. 4.8).

4.4.3.1 Topic Selector

When clicking the "Assessment" button of a case panel on the dashboard, a *Topic Selector* page will be shown which visually represents the assessment questions applicable to the case, structured by assessment tasks (top bar), topics (sub-panel headings), aspects (sub-panel content), and the number of questions for each aspect (Fig. 4.11). A user can now pick any of those elements in order to filter assessment questions presented in the subsequent assessment view (Fig. 4.12).

The page further provides individual progress indicators for each task subset. This is useful for managing the assessment workload, as a case may possibly involve hundreds of assessment questions to address, and a user can so focus on a particular subject or task, and return later to select another.


ASSESSMENT
ABANDONED BAGGAGE DETECTION

FUNCTION: Assessment Leader
ROLE: SMT Investor

Completion Progress (1 / 2)

FILTER

Choose Task: Assessment of Legal Is:

Choose Topic: Bodily integrity

Choose Aspect: Distribution

QUESTIONS BY TOPIC

Discrimination based on a personal characteristic?

Discrimination based on a circumstantial (non-personal) characteristic - arbitrary or reasonable?

Discrimination based on a personal characteristic?

Bodily integrity and Distribution

The question which grounds for differential treatment fall under the protection of Art. 14 ECHR is subject to controversy. It is undisputed that the grounds named explicitly in Art. 14 ("sex, race, colour, language, religion, political or other opinion, national or social origin, association with a national minority, property, birth") are protected. Moreover the case law of the ECtHR indicates that also any other "personal characteristic is protected. A "personal characteristic" is something that relates directly to the individual and is not just a circumstantial characteristic. However, the boundary between what is personal and what is not, is fuzzy. To add to the confusion some of the case law of the ECtHR seems to indicate that the protection of Art. 14 is not limited to "personal characteristics" but offers a full-blown equal treatment protection, covering all possible grounds for differential treatment. See: Gerards, J. (2013). "The Discrimination Grounds of Article 14 of the European Convention on Human Rights." On the definition of "personal characteristic" see e.g.: ECtHR, Clift v. UK, no. 7205/07, 13 july 2010.

Is the discriminatory distribution of the enjoyment of the protection of bodily integrity based on (direct discrimination) or correlated to (indirect discrimination) a personal characteristic?

○ Yes ○ No

Justify your answer:

Fig. 4.12 SIAM AST – main assessment tool

4.4.3.2 Main Assessment Tool

The assessment view shown in Fig. 4.12 presents a feature-rich tool for actors to engage in technology impact assessment. On the left-hand side, user can work with filters to constrain how many assessment topics to work with at the same time.[38] Underneath is an interactive navigation tree, displaying the currently selected subset of topics, aspects, and questions in a hierarchical fashion. Questions that appear in grey colour are conditional – these will only be activated once certain answers have been given to previous questions. Questions which have been answered will be ticked off and appear in a green colour in this tree, and an increasing number of answers recorded will be reflected by the progress bar located in the top-left corner.

The middle section of the page in Fig. 4.12 displays information around the actual assessment issue such as associated topic and aspect, an explanatory text and the actual question. Further, relevant answer options are offered. An answer may constitute a textual answer, or selecting a multiple choice option, combined with a textual justification or explanation of the answer chosen. User can use the arrow-buttons to the left and right of this section to cycle through the available questions.

[38] The filters provide the same constraining functionality (tasks, topics, aspects) as the *topic selector*, however they are much quicker to use and intended for pro-users who acquired a certain routine in using the tool.

On the right-hand side, additional tools that are relevant in this context are provided. For instance, users can inspect supplementary resources that are provided with the question (like methodological advice, or legal reference texts, for example). They can also attach a document themselves as part of their answer, like a report or a diagram. Users can also send delegation requests to other actors, asking them to answer a particular question which they are unable to answer themselves. Moreover, every user may create their own, custom questions, which allow them to address issues that are more specific to the current case, and add these to the question pool. Custom questions can be targeted at other (single) actors, or alternatively, at all invited actors of a particular role (e.g., all actors of the role "Data Protection Authority").

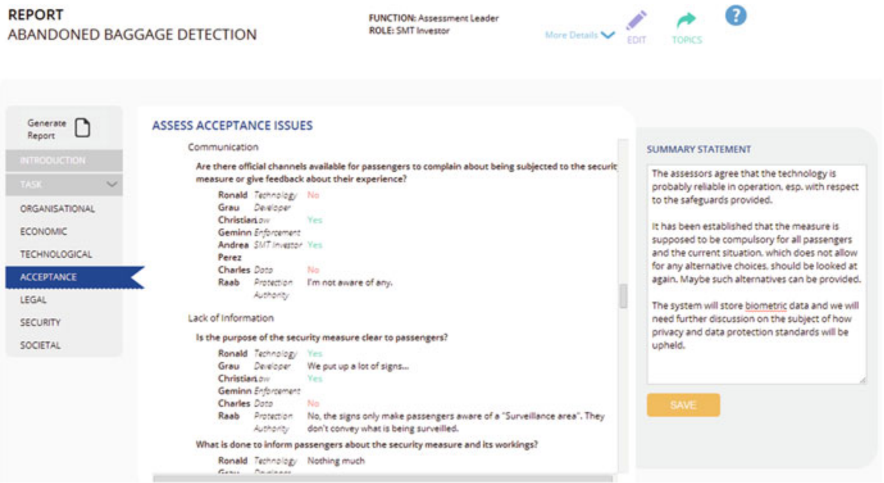
4.4.4 Analysis and Reporting

An assessment leader of a case can edit and compile an assessment report for that case at any time. The report draws together the contributions made by all invited actors, documents any summary statements and resources supplied in a structured fashion, and provides further guidance on how to improve the assessment.

4.4.4.1 Report Customisation Tool

Before creating a report, the assessment leader of a case will first use a tool that offers a preview of the report chapters. The introductory chapter is partially prepopulated with the information provided during assessment case configuration, in particular details about the scenario, the assessed technology, and the participating actors. The editing user can add an additional section here to customise the introduction contents as required. Further, the report customisation tool will lists all assessments made by the individual actors, ordered by task, topic, and aspect, offering visual cues for the assessment leader to identify those areas where the actors agree, those where there are conflicting views, and those which have not been sufficiently addressed yet. The assessment leader can then summarise the current situation for the issues discussed within a chapter issue with a short statement. Figure 4.13 shows a screen shot of this tool which illustrates an example concerning some of the assessment issues which are to appear in an "Acceptance" section of a report.

Depending on the size of the question pool, a single assessment case may involve thousands of assessment questions in need to be addressed, and the SIAM AST as a web-based system can handle a huge number of users getting involved to contribute their expertise and opinions on these topics. These capabilities present one of the major strengths of the system but reveal a weakness at the same time, as the effort for summarising and evaluating the contributions will get increasingly time-consuming as impact assessments are made more inclusive and balanced in terms of the kinds



REPORT
ABANDONED BAGGAGE DETECTION

FUNCTION: Assessment Leader
ROLE: SMT Investor

ASSESS ACCEPTANCE ISSUES

Communication

Are there official channels available for passengers to complain about being subjected to the securit measure or give feedback about their experience?

Ronald Grau Technology Developer No
Christian Law Yes
Geminn Enforcement
Andrea Perez SMT Investor Yes
Charles Raab Data Protection Authority No I'm not aware of any.

Lack of Information

Is the purpose of the security measure clear to passengers?

Ronald Grau Technology Developer Yes We put up a lot of signs...
Christian Law Yes
Geminn Enforcement
Charles Raab Data Protection Authority No No, the signs only make passengers aware of a "Surveillance area". They don't convey what is being surveilled.

What is done to inform passengers about the security measure and its workings?

Ronald Grau Technology Developer Nothing much

SUMMARY STATEMENT

The assessors agree that the technology is probably reliable in operation. esp. with respect to the safeguards provided.

It has been established that the measure is supposed to be compulsory for all passengers and the current situation. which does not allow for any alternative choices. should be looked at again. Maybe such alternatives can be provided.

The system will store biometric data and we will need further discussion on the subject of how privacy and data protection standards will be upheld.

Fig. 4.13 SIAM AST – assessment report customization tool

and number of actors involved. While human judgment on many of the complex issues at the heart of technology impact assessments may be considered superior over the capabilities of current computational approaches, a solution is needed for managing the cognitive workload invoked by such assessments. The report customisation tool shown in Fig. 4.13 makes some initial effort in this direction by providing perceptual cues that enable a user to navigate the structured information and recognise quickly the state of each topic addressed. Nevertheless, the means employed here are very basic. Alternative approaches to thoroughly capture and structure the underlying information could be realised by the application of other, advanced knowledge engineering and modelling methods,[39] and the development of innovative, representational systems and tools.[40,41]

4.4.4.2 Assessment Report and Scoring

The assessment report is essentially a snapshot of the current state of an assessment. It can be created at any time and used to track progress, document new evidence,

[39] E.g., T.J. Menzies. "Knowledge Elicitation: the State of the Art", in: *Handbook of Software Engineering and Knowledge Engineering*, Volume II. 2002.

[40] E.g., P.C-H. Cheng and R. Barone, Representing complex problems: A representational epistemic approach. In Jonassen, D.H. (ed.), *Learning to solve complex scientific problems*, (Mahmah, N.J., Lawrence Erlbaum Associates, 2007), 97–130.

[41] For instance, by using diagrammatic knowledge-based systems: Ronald Grau and P.C.-H. Cheng, "The Support of Higher-level Cognition in the Context of Ill-structured Process Knowledge", 2nd Annual Conference on Advances in Cognitive Systems, (Baltimore, MD, 2013).

and audit any evaluations made. From top to bottom, it contains relevant dates, and a title and introductory chapter detailing the problem context, the technology assessed, and actors involved in the assessment. Further, there are sections for each assessment task, which present the summary statements made by the assessment leader on different assessment topics. A separate section with a range of assessment scores is followed by a large appendix, detailing all assessment questions posed to the actors, and the different answers received.

With respect to the example assessment scores implemented in the prototype, the software takes attributes of the *questions* asked (count, perspective, task), as well as attributes of the *answers* given (count, associated actors) to calculate different scores, and include these in the assessment report. Independent of the type of score, each is presented as (1) a global score, based on the entire question pool applicable to the case; (2) Differentiated by Assessment Perspectives; and (3) Differentiated by Assessment Tasks (Fig. 4.14).

Completion Score

This is a basic measure, indicating how many assessment questions from a given set have been addressed by at least one actor. The calculation is based on the non-conditional questions shown for each topic and aspect. If every question in the subset has received at least one answer, the score will be 100 %. Calculation:

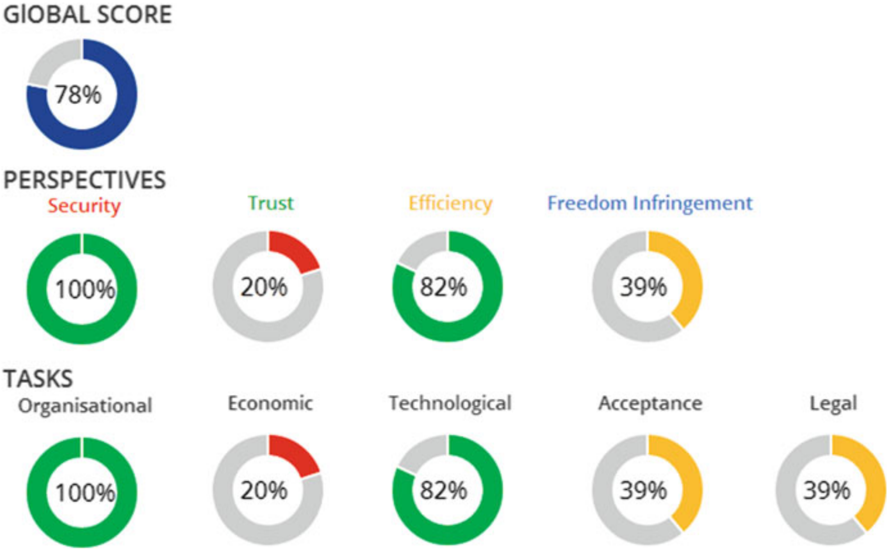


Fig. 4.14 Partial screenshot of a scoring section in the SIAM assessment report

x: The count of answers given for any non-conditional questions of the case
divided by
y: The count of all non-conditional questions that would be posed in the case.

Involvement of Actors Score

This score takes the number of actors with distinct roles which have been invited to a case, and compares this to the number of distinct roles at which the particular set of assessment questions are targeted. Also, concrete (textual) suggestions are made as a result as to which roles are currently missing from the case to achieve a more balanced assessment. Calculation:

x: The count of distinct roles that have been invited * count of non-conditional questions they would see
divided by
y: The count of distinct roles that each non-conditional question was targeted at * count of those questions.

Participation Score

This score looks at the number of answers given by actors of distinct roles and compares this to the number of distinct roles which should have answered those questions, based on the actual set of actor-roles invited to the case. The score calculates the extent to which assessments are based on limited views because not all roles present have contributed answers. This can be useful to decide whether the invited actors should be encouraged to actively contribute their views on all the issues posed to them. Calculation:

x: The count of distinct roles that have answered * count of non-conditional questions posed
divided by
y: The count of distinct roles that have been invited * count of non-conditional questions the related users would see.

The basic scores developed for the SIAM AST demonstrate how semantic attributes attached to components of an assessment process can be exploited to guide assessment activities, independent of the actual technology considered. Naturally, these scores could be further differentiated to monitor the course of an impact assessment on finer levels of detail. The use of other semantic tags would also facilitate additional scores.

4.5 Evaluation

The evaluation of the software was conducted in an iterative fashion, with several consecutive stages during and after development. These were realised as a series of workshops (10 in total over the course of two years), where a range of real end users evaluated the structure and functionality of the assessment support toolkit in its respective development state. Each such session usually involved an initial presentation of the core concepts and functions of the system, followed by an interactive session where the participants operated the software to jointly work on one more example assessment cases, the collective inspection of the results, and finally a discussion. The events involved a wide spectrum of prospective end users from various European countries. Their professional background included technology developers, police representatives at the state or federal level, data protection authorities at the state level, lawyers, security managers of airport and railway facilities, security measure operators, academics, human rights organisation representatives, private security companies, and members of private research organisations. Evaluation information was elicited by means of questionnaires which the participants completed during the workshops, as well as open feedback given in writing or during the discussion. The questions explored issues concerning the usefulness of the system, its particular features, and how these were embedded and interconnected to support the assessment workflow; the suitability of the concepts developed, the usability of the interfaces, or the applicability of assessment content, for example.[42]

The *first* evaluation stage consisted of three smaller user fora, involving participants from Germany, Italy, and Israel, who tested a first wireframe version of the toolkit.[43] Based on the results gathered, a first prototype of the actual system was specified and developed and then evaluated again in a *second*, larger user forum, with a diverse set of more than 30 participants from different European countries involved.[44],[45] The *third* and most recent stage of evaluation comprised a series of

[42] It is not possible to present detailed results within the space of this chapter but references have been provided to the respective reports, where possible. Due to the iterative nature of the evaluation process, many of the earlier results are also somewhat implicit in the final version of the prototype presented in Sect. 4.4.

[43] A wireframe is a rapidly produced prototype with limited functionality that is commonly used for illustrating features in the early stages of software development. For details of the results see Andreas Timmermann, “User Forum Report”, SIAM Deliverable D 13.11, (European Commission, 2012).

[44] For details, see Graeme Jones, Ronald Grau, and Hans Lammerant, “Updating the SIAM Application Requirements: Freedom Infringement; AST tool development activities”, SIAM deliverable D8.2, (European Commission, 2013).

[45] For more details on the evaluation, see Leon Hempel, Lars Ostermeier, and Tobias Schaaf, “The SIAM User Forum, Report”, SIAM Deliverable 13.12, (European Commission, 2013).

five local workshops, conducted with participants from Belgium, Germany, Italy, Israel, and the UK in March 2014.[46]

Overall, participants thought the toolkit presented an interesting and useful approach to assessing technology from different angles, and involving several relevant actors easily. For example, participants at a most recent workshop suggested to "*promote the system as a support to design for data protection by default*", that "*the system is objective and one can very easily take in account human rights*", or "*the system is user-friendly and generates good as well as clear statistics*".[47] Others emphasised the usefulness for automated and structured recording of evidence and documentation, for making actors accountable for their decisions, and that the interface is intuitive to use. There were also other, conflicting statements (e.g., to have more content, but less workload at the same time), or the desire to include content that would be challenging to integrate (e.g., question content that considers both national and international law). As was expected, opinions sometimes differed between participants with different roles, or cultural or national backgrounds. Interestingly, some desired that "*The system should allow the participants to see each other's answers*", as this was intentionally designed to be only possible in the reports, in order to avoid bias during assessment. Across the board, the participants valued highly that the question content is independent from the software such that additional and even entirely different questions can be created to be employed by the system, using the authoring facilities offered.[48] Finally, it was observed that participants usually had no or little difficulties using the supplied communication features for messaging, creating custom questions, or delegating questions to other actors as part of the general work flow.

Whilst these workshops yielded encouraging first results, the system needs to be applied in a real application context for a more comprehensive evaluation. Also, the system is currently a prototype which, although entirely functional, needs further refinement to be entirely applicable and capable to deal with other technology assessment problems, outside the contexts of security, data protection, or mass transportation for that matter. Overall, this work was successful in delivering an approach and implementation for a complex problem that demonstrates the exciting opportunities that assessment support systems can offer.

4.6 Summary

Models and tools underpinning a computational assessment support toolkit were discussed in this chapter. The tools support the high-level monitoring and guidance of technology impact assessments (TIA) in the context of security technology

[46] E.g., some specific results are in Ekaterina de Vries and Veerle Pashley, "Report of the SIAM Workshop (Vrije Universiteit Brussel)", SIAM Deliverable 13.17, (European Commission, 2014).

[47] Ibid., 3.

[48] De Vries and Pashley, "Report of the SIAM Workshop (Vrije Universiteit Brussel)", 5.

planning and acquisition processes in mass transportation sites. This development addresses important problems related to the (1) Integration of different assessment perspectives and tasks in the evaluation of technological solutions; (2) Availability, distribution, and reflexivity of relevant information and knowledge among the various stakeholders and actors involved; (3) Accountability of actors with regard to their individual assessments; (4) Auditability of supplied evidence and documentation.

The SIAM AST demo software is intuitive to use and offers a web-based platform for creating and managing assessment cases for different technological solutions which are proposed to solve particular security problems. Decision-makers can involve relevant actors to assess the various impacts that could materialise as a result of implementing a proposal, even if the actors live geographically apart. The current software prototype employs a sample pool of assessment questions (open to extension) that address many relevant issues, including technological, economic, organisational, and legal concerns; issues related to the infringement of human rights and liberties; ethical considerations, and possible acceptance problems related to a security measure or technology. The toolkit provides a rich set of assessment, documentation, and communication features, integrated into a systematic assessment support process. This process facilitates the collection and storage of evidence and makes transparent to all actors the different views and perspectives in the spectrum of assessment topics. It can help identify and mitigate major problems that could occur during or after the implementation of a proposal, and minimise the additional cost or chance of failure that may emerge in the course of attempts to resolve such problems within or after the implementation phase. For instance, problems may be foreseen which would otherwise require compromises or trade-offs to be made later, which might jeopardise the usefulness, legitimacy, or effectiveness of a solution overall.

Bibliography

"A Global Approach for European Civil Aviation Security", White paper, Version 1.0, (EOS Civil Aviation Security Working Group 2009).

Annex 17 to the Convention on International Civil Aviation – Security – Safeguarding International Civil Aviation against acts of unlawful interference, Ninth edition, (International Civil Aviation Organization, 2011).

Cheng, P.C.-H., Barone, R. (2007). Representing complex problems: A representational epistemic approach. In Jonassen, D.H. (ed.), Learning to solve complex scientific problems, Mahwah, N.J., Lawrence Erlbaum Associates, pp. 97–130.

"Cost Explosion: Price Tag for New Berlin Airport Keeps Rising", accessed March 1, 2014, http://www.spiegel.de/international/germany/5-billion-euros-costs-increase-again-for-berlin-brandenburg-airport-a-928989.html.

De Vries, Ekaterina, and Veerle Pashley, "Report of the SIAM Workshop (Vrije Universiteit Brussel)", SIAM Deliverable 13.17, European Commission, 2014.

European Commission – CORDIS – Projects – SIAM, accessed March 1, 2014, http://cordis.europa.eu/projects/rcn/97990_en.html.

Fenz, Stefan, and Andreas Ekelhart, "Formalizing information security knowledge", in: *Proceedings of the 2009 ACM symposium on Information, computer and communications security*. (ACM, New York, 2009).

"German defense minister to face grilling over Euro Hawk debacle", accessed March 1, 2014, http://www.dw.de/german-defense-minister-to-face-grilling-over-euro-hawk-debacle/a-16964646.

Grau, R.R. and Cheng, P.C.-H., "The Support of Higher-level Cognition in the Context of Ill-structured Process Knowledge", 2nd Annual Conference on Advances in Cognitive Systems, Baltimore, MD, 2013.

Grau, Ronald, and Graeme Jones, "The SIAM Assessment Support Toolkit: A Software System for the Support of Technology Impact Assessments", SIAM deliverable D11.2, European Commission, 2014.

Hempel, Leon, Ostermeier, Lars, Schaaf, Tobias and Dagny Vedder, "Innovation Journey Report", SIAM deliverable D2.4, European Commission, 2011.

Hempel, Leon, Grau, Ronald, Ostermeier, Lars, Schäufele, Fabia, Schaaf, Tobias, and Dagny Vedder, "SIAM – Security Impact Assessment Measures. Ein System zur Unterstützung von Security Technology Assessments an Flughäfen und im öffentlichen Nahverkehr", Oranienburger Schriften, Fachhochschule der Polizei des Landes Brandenburg, 2011.

Hempel, Leon, Ostermeier, Lars, and Tobias Schaaf, "The SIAM User Forum, Report", SIAM Deliverable 13.12, European Commission, 2013.

Jones, Graeme, and Ronald Grau, "A Typology of Security Measure Technologies and Counter Infringement Technologies", SIAM deliverable D2.3, European Commission, 2012.

Jones, Graeme, and Ronald Grau, "The SIAM Assessment Support System: Initial Application and Database Specification", SIAM deliverable D11.1, European Commission, 2012.

Jones, Graeme, and Ronald Grau, "Updating the SIAM Application Specification from WP6", SIAM deliverable D6.4, European Commission, 2012.

Jones, Graeme, and Ronald Grau, "Updating the SIAM Application Requirements: Crime-modelling and ASS tool development activities", SIAM deliverable D7.3, European Commission, 2013.

Jones, Graeme, Grau, Ronald, and Hans Lammerant, "Updating the SIAM Application Requirements: Freedom Infringement; AST tool development activities", SIAM deliverable D8.2, European Commission, 2013.

Marakas, George M., *Decision support systems in the twenty-first century,* Upper Saddle River, N.J., Prentice Hall, 1999.

Menzies, T.J., "Knowledge Elicitation: the State of the Art", *Handbook of Software Engineering and Knowledge Engineering*, Volume II, 2002.

Regulation No. EC 300/2008 on common rules in the field of civil aviation security, accessed March 1, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:097:0072:0084:EN:PDF.

Sharan, Yair, Rosenberg, Shlomo, Tzesana, Roey, Verfaillie, Kristof, Boyle, Phil, Migliorini, Massimo, and Christian L. Geminn, "Threat Scenarios Report", SIAM deliverable D6.3, European Commission, 2012.

Sommerville, I. Software Engineering, 7th ed. Harlow, UK: Addison Wesley, 2006.

"The curious case of Berlin's Brandenburg Airport: Will it ever open?", accessed March 1, 2014, http://www.newstatesman.com/business/2013/09/curious-case-berlins-brandenburg-airport.

Timmermann, Andreas, "User Forum Report", SIAM Deliverable D 13.11, European Commission, 2012.

Van de Ven, Andrew, Polley, Douglas, Garud, Raghu and Sankaran Venkataraman, *The Innovation Journey*. (New York: Oxford University Press, 1999).

Verfaillie, Kristof and Rosamunde van Brakel, "Assessing security threats in mass transportation sites", SIAM Deliverable 6.2, European Commission, 2012.

Chapter 5
Impact Assessments as Negotiated Knowledge

Leon Hempel and Hans Lammerant

Abstract The existing literature on privacy impact assessments (PIA) considers such instruments as tools to produce knowledge and as part of risk management. This article wants to reconsider impact assessments as political tools, in which knowledge production can not be separated from negotiations between interests.

First impact assessments are situated in the account of Ulrich Beck's Risk Society. Beck points to the decentralization of political decision making and the development of subpolitics. Impact assessments are an example of a tool to democratize subpolitics. Secondly the typology of environmental impact assessments from Cashmore is introduced to consider how the purpose given to impact assessments, varying from informing over influencing decision making to co-decision making, is related with the role given to knowledge and to stakeholder involvement. Which knowledge is relevant is shown to be negotiated in an interest-driven context.

The last part shows that awareness of the political nature of impact assessments also helps to approach the problem of integrating various disciplines. The relation between different disciplines in an impact assessment is not fixed. An impact assessment is a political process and has its own mechanism of closure defining what is a relevant impact and relevant knowledge about them.

Impact assessments are often understood as instruments to bring some rationality into decision making processes concerning controversial policies and projects. But at the same time they are not just neutral tools to produce a certain knowledge to inform decision makers, but always political according to the way they are shaped and formalized, according to what role science or different scientific disciplines may play, and how and by whom definitions are made, adopted and contextualized during the assessment project. The knowledge produced, i.e. the final assessment output, is not a simple truth about an impact of a considered project. It itself is a result of

L. Hempel
Centre for Technology and Society (CTS), Technical University of Berlin, Berlin, Germany
e-mail: hempel@ztg.tu-berlin.de

H. Lammerant (✉)
Law Science Technology & Society (LSTS), Vrije Universiteit Brussel, Brussels, Belgium
e-mail: hans.lammerant@vub.ac.be

S. Gutwirth et al. (eds.), *Reforming European Data Protection Law*,
Law, Governance and Technology Series 20, DOI 10.1007/978-94-017-9385-8_5

the widespread negotiations on what has been seen and conceptualized as a relevant impact in the first place. It is thus an outcome of value discussions and interests.

The following article reconsiders the relation of knowledge and power within impact assessments. It mainly derives from the observation that in the literature on data protection, privacy, surveillance or any other related impact assessment on novel technologies, there is hardly any explicit consideration of this relation. In the area of Environmental Impact Assessment (EIA) the debate on the role of knowledge and power has been going on for much longer and it seems reasonable to review some of the lessons learned in the area of data protection, privacy and surveillance. However, taking into account the high expectations towards impact assessments in these areas, it seems appropriate to do so in order to prevent expectations from becoming too optimistic.

We first aim to situate impact assessments as a regulatory technique in the context of Ulrich Beck's risk society. Especially, his notion of subpolitics as forms of politics beyond the traditional institutions of representative democracies will allow us to investigate the reasons as well as implications behind the emergence and the ever-growing proliferation of impact assessments. In the second part we will reflect on the role of science and the relation between power and knowledge in order to show how this relation actually affects the undertaking of impact assessments, the formation of purposes, procedures and outcomes. The discussions and experiences given in the literature on EIAs will give us highly important insights for this. In the last part we look at what this means for the integration of different disciplines.

5.1 Situating Impact Assessments as Subpolitics

Impact assessments are tools of growing popularity. Since their first appearance as environmental impact assessments in 1970, namely in the US National Environmental Policy Act (NEPA), they have proliferated as a regulatory technique in other areas. A whole range of different approaches exist such as Constructive Technology Assessment (CTA), Real Time Assessment, Social Impact Assessment (SIA)[1] and so on. These imply certain foci in terms of purposes, procedures or impact dimensions, but also overlap in many respects.[2] Moreover, impact assessments have

[1] See for the different approaches: Schot, Johan und Arie Rip 1997, The Past and Future of Constructive Technology Assessment. *Technological Forecasting and Social Change* 54 (2–3): pp. 251–268. Guston, David H. und Daniel Sarewitz 2002, Real-time technology assessment. *Technology in Society* 24: pp. 93–109 and Vanclay, Frank, "International principles for social impact assessment", *Impact Assessment and Project Appraisal*, Vol. 21, No. 5, 2003, pp. 5–11.

[2] For an overview on different assessment approaches see: Barbara Prainsack, Lars Ostermeier, *Report on methodologies relevant to the assessment of societal impacts of security research*, D 1.2 Assert-project, http://assert-project.eu/wp-content/uploads/2013/04/ASSERT_D1.2_KCL_final.pdf.

captured the field of data protection, privacy and surveillance. Different approaches exist and diverse guidelines are at hand.[3] In our view this proliferation as a whole must be seen as exemplary for a broader social change regarding the meanings and roles science and technology play in society and how both can be regulated. To gain a better understanding of this proliferation as well as of the meaning of impact assessments we begin by situating it under the notion of reflexive modernization as Ulrich Beck has coined it in his famous book Risk Society.[4]

In his book, Beck points to the changing conflicts arising as side effects of on-going techno-economic development. While the welfare state ameliorated the many miseries that industrialization and the logic of wealth distribution had come to mean, especially for the working class during the nineteenth and first half of the twentieth century, another source of conflict arose in the 1960s: risks due to environmental pollution, health risks for consumers, etc. However, the major difference of these side-effects was that they were produced by technological and scientific progress itself. Science and modernity are not simply struggling against tradition and natural scarcity, but also against the danger produced by themselves.[5]

> We are therefore concerned no longer exclusively with making nature useful, or with releasing mankind from traditional constraints, but also and essentially with problems resulting from techno-economic development itself. Modernization is becoming *reflexive;* it is becoming its own theme. Questions of the development and employment of technologies (in the realms of nature, society and the personality) are being eclipsed by questions of the political and economic 'management' of the risks of actually or potentially utilized technologies – discovering, administering, acknowledging, avoiding or concealing such hazards with respect to specially defined horizons of relevance. The promise of security grows with the risks and destruction and must be reaffirmed over and over again to an alert and critical public through cosmetic or real interventions in the techno-economic development.

Scientific progress is no longer just the producer of societal benefits but also of dangers to society. The result is a shift within the relation of science and the public but also within science itself. Reflexive modernization implies the turning of science's methodological skepticism to science itself. As the producer of risks it immediately discovers its role to discern the risks it has produced and starts a "process of demystification", in which "the structure of science, practice and the

[3] David Wright and Paul De Hert (eds), *Privacy Impact Assessment*, (Dordrecht Heidelberg London New York: Springer), 2012; Wright, David, and Charles D. Raab, "Constructing a surveillance impact assessment", *Computer Law & Security Review* 28 (2012): 613–626. Wright, David, and Kush Wadhwa, *A step-by-step guide to privacy impact assessment. Empirical research on contextual factors affecting the introduction of PIA frameworks in EU Member States*, Poland, April 2012. Available at: http://www.piafproject.eu/ref/A_step-by-step_guide.pdf.

[4] Ulrich Beck, *Risk Society, Towards a New Modernity*. Translated by Marc Ritter, London, Newbury Park, New Delhi: Sage Publications, 1992.

[5] Beck, *Risk Society,* p. 19–20.

public sphere is subjected to a fundamental transformation".[6] At the same time its knowledge monopoly is scrutinized. Traditionally seen to be the uneducated receivers of scientific wisdom, or even worse, people with naïve beliefs, the public begins to question the role of science and scientists in society. Scientific research is not an unquestionable good anymore but now has to legitimate itself.[7]

In this respect impact assessments gain significance. Their proliferation can be seen both as an expression of, and a method for dealing with the increasing demand of legitimization by introducing reflexivity into techno-scientific processes. Even when impact assessments are done by a limited group of experts, it shows that the projects under consideration cannot be seen simply as unquestionable signs of progress, but now must supply justification beyond their own implicit normativity. The turn to participatory approaches in impact assessments then deepens the reflexivity and pulls experts and scientists further into the legitimacy debate including those scientists, e.g. social scientists, who are carrying out the assessments themselves.[8]

However, the shift from the logic of wealth to that of risk distribution also has implications for the political landscape. In the risk society the grip of the formal political institutions on society lessens and new forms of politics outside and beyond traditional politics proliferate. In the arenas of subpolitics other societal actors outside parliaments and governments gain impact, challenge conventional decision-making and thus transcend the formal political system in its practices, orientation and rules of decision-making. The de-monopolization of scientific truth is accompanied by a decentralization of political acting. It is a highly ambivalent process. On the one hand subpolitics can compensate political gaps, on the other they often stay hidden from view. Indeed, new hybrid monopolies, consisting of state as well as of non-state actors, emerge beyond democratic control. Industry and science attain an enormous impact while the formal political institutions fail to impact both.

In the end techno-scientific research occurs on a highly deregulated level while technological developments often have a large and unpredictable impact on society, an impact larger even than that of legislation. It becomes difficult and even impossible to regulate future technological developments through law. Technological developments leave law and politics behind. Law and politics do not control these developments, but are confronted with their consequences. Formal political institutions still reflect the idea of a central command and control over societal developments, while the actual power of these institutions is diminishing.

[6] Beck, *Risk Society,* p. 156.

[7] Beck, *Risk Society,* p. 175.

[8] See: Macnaghten, Phil, Matthew B. Kearnes and Brian Wynne, Nanotechnology, Governance, and Public Deliberation: What Role for the Social Sciences? *Science Communication* 27 (2005): pp. 268–291. Williams, Robin 2006, Compressed Foresight and Narrative Bias: Pitfalls in Assessing High Technology Futures. Science as Culture 15 (2006): pp. 327–348.

Instead, new social movements, non-governmental organizations and citizen groups are gaining voice and are beginning to play an increasing role in new political arenas. Even though this process of decentralization of politics implies in part more freedom for social movements and citizens as the monopoly of traditional politics wanes, all these forms of subpolitics[9] are not – by definition – democratic. Especially industry and scientific research work remains more or less a closed world that is increasingly independent and based on its own rationality.

Borrowing from Gunther Teubner, Thomas Mathiesen has talked of a *lex vigilatoria* of a globalized surveillance and security realm. As the *lex mercatoria*, its equivalent in the economic sphere, the *lex vigilatoria* is developed outside the central political institutions and given sanction by parliaments. The *lex mercatoria* has been developed "through the work of the large and expanding group of professional lawyers operating on the transnational level, tying vast capital interests together in complex agreements furthering capital interests". Similarly the *lex vigilatoria* is developed by system functionaries working on "integrated or 'interlocked'" information systems, which are at the same time "increasingly becoming untied or 'de-coupled' from the nation-states". Decision-making in these arenas becomes "self-referential and self-validating".[10] Neither political institutions and their democratic organization of policy debate, nor other societal actors gain a meaningful possibility to question them or to have a direct impact on scientific-industrial work. Especially "techno-economic sub-politics" tend to seclude themselves. Already Beck observed[11]:

> Decision-making on techno-scientific development and its economic exploitation, however, escapes the reach of research policy. In relations to the state, industry possesses a double advantage, that of the *autonomy of investment decisions* and the *monopoly on the application of technology.* The strings controlling the modernization process in the form of economic planning, of the economic yield (or risk) and of the technological structure in the firms themselves all lie in the hands of economic sub-politics.

However, the term subpolitics also offers a different view on 're-politicization', different from pushing the matter back into the old formal political institutions. Despite its implicit threat of political vacuity, it opens a view on re-politicization which is more decentralized and consists of opening up forms of more active decision making. Within the tendency of decentralization of the political process, impact assessments can be understood as a form of subpolitics. In fact, an

[9] Boris Holzer and Mats P. Sorensen talk of "the passive and the active side of subpolitics as well as their possible interaction" to demonstrate the spectrum as whole. See: Holzer, B. and M. P. Sorensen: Rethinking Subpolitics. Beyond the 'Iron Cage' of Modern Politics? Theory, *Culture & Society* April 2003 vol. 20 no. 2 79–102.

[10] Thomas Mathiesen, Lex Vigilatoria – Towards a control system without a state?, in: Deflem, Mathew (ed.) *Surveillance and Governance: Crime Control and Beyond,* Bingley, Emerald Group Publishing Limited, pp. 101–130.

[11] Beck, *Risk Society,* p. 212.

ever-accelerating technological evolution makes it increasingly difficult to assess and regulate potential impacts of novel technological projects. As such, impact assessments also reflect the ongoing crisis of policy-making.[12] The complexity of potential consequences and thus the risks are beyond comprehensive regulative instruments such as the law or political decision-making processes. In this respect, one could argue that the use of impact assessments is – at least in part – a method to delegate the power to regulate socio-technological change in an absence of better options. Within a general legal framework with some guiding norms, regulative power is delegated to project developers in order to negotiate solutions specific for the project based on an expertise that goes beyond the mere technological perspective. Elite models, based on highly qualified experts can be differentiated from democratic models, in which the general public plays a significant role.[13] Depending on how impact assessments are implemented, they become a method to de-politicize decision-making or to organize the political debate around technology and its uses in a more decentralized manner.

When impact assessments are made mandatory as part of public inquiry procedures or as a distinct obligation before implementing a project as in environmentalism, legal rules install a framework for debate. These instruments are tools to produce a certain knowledge, about 'the environmental effects' of a project or 'the impact of the envisaged processing operations on the protection of personal data', but as this legal framework shows, these tools are primarily political instruments introducing into decision-making a method to deal with the legitimacy of the project and to make decisions more accountable. The legal framework specifies the minimal information to be provided and, as a consequence, also the minimal issues to be considered, and an explicit account of how they will be dealt with. By making consultation of the concerned public obligatory, it gives stakeholders a legal standing to raise questions during the impact assessment or the decision-making process, and forces the project developers and involved experts to answer their concerns.[14] Thus, this legal framework institutionalizes subpolitics to a certain degree. Indeed, the turn to participatory approaches can be seen as an example of democratization in this form of subpolitics.

[12] See: Alonso, Sonia et al., *The Future of Representative Democracy*, (Cambridge: Cambridge University Press 2011); Michaelsen, Danny, Franz Walter, *Unpolitische Demokratie. Zur Krise der Repräsentation*, (Berlin: Suhrkamp 2013), especially pp. 179 on the process of de-parliamentization of politics and deliberative surrogate-democracy since the 1970s.

[13] Prainsack and Ostermeier, *Report on methodologies relevant to the assessment of societal impacts of security research*, p. 20.

[14] See for EIA the Directive 2011/92/EU of 13 December 2011 on the assessment of the effects of certain public and private projects on the environment; for DPIA/PIA see article 33, 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/2012/011 final – 2012/0011 (COD).

5.2 The Politics of Impact Assessments, or, Have We Adequately Considered the Relation Between Knowledge and Power?

Understanding impact assessments as subpolitics emphasizes the need to reconsider the relation between knowledge and power or interests. Already the term impact is obviously not a value-free notion but a construction of what is selected as relevant. For instance, while a Privacy impact assessment has a normative focus on privacy, a Surveillance impact assessment focuses on the *societal* implications of surveillance. Accordingly, "it must address the impacts of a surveillance project not only on privacy, but also on other issues and impacts e.g. social, economic, financial, political, legal, ethical and psychological". What is actually at stake can thus be defined differently and presumably depends not only upon the project's application context but also upon the scientific and political standpoint of the expert and the interest of those who initiated the process in the first place.

In the literature impact assessments are mainly presented as tools to produce knowledge for informed decision-making, and are most often conceptualized as risk assessments. Wright points out that they are often described as an "early warning system"[15] and in fact, looking at guideline PIAs, follow core risk assessment procedures.[16] Based on a review of various PIA definitions, Wright and De Hert define the idea of PIA: It "is a process for identifying and evaluating risks to privacy, checking for compliance with privacy legislation and considering ways in which those risks can be avoided or mitigated."[17] Within various steps of planning, negotiating and documenting, the main focus remains to 'identify risks and possible solutions.'[18] However, the term risk also presumes a normative horizon and its definition, as Beck pointed out, again has ethical and political implications. "Statements on risk are the moral statements of scientised society".[19] According to Brian Wynne the notion of risk has meanwhile become "the defining discourse identifying the meaning of

[15] David Wright, The state of the art in privacy impact assessment, 2012 *Computer Law & Security Review* 28 (2012), p. 55.

[16] Spiekermann, Sarah, The RFID PIA – developed by industry, agreed by regulators, in: David Wright and Paul De Hert (eds), *Privacy Impact Assessment*, (Dordrecht Heidelberg London New York: Springer, 2012), pp. 323–346.

[17] Wright, David, and Paul De Hert, "Introduction to Privacy Impact Assessment", in: David Wright and Paul De Hert (eds), *Privacy Impact Assessment*, (Dordrecht Heidelberg London New York: Springer, 2012), p. 7

[18] Wright, David, and Kush Wadhwa, A step-by-step guide to privacy impact assessment. Empirical research on contextual factors affecting the introduction of PIA frameworks in EU Member States, Poland, April 2012. Available at: http://www.piafproject.eu/ref/A_step-by-step_guide.pdf.

[19] Beck, *Risk Society*, p. 176.

public issues concerning scientific research and development".[20] In a "monovalent simple-realist discourse [. . .] the risks, though they may be imprecisely known, have a meaning which is taken for granted, not a political-cultural artefact whose meaning and definition have been (deliberately or not) *constructed*."[21]

In respect to its universality the risk discourse forms subjects and cultures, including a hegemonic Western-developed scientific culture, which "implicitly" imposes "saliency or irrelevance of local contextual conditions". It produces a "standardized model of the citizen"[22] as Wynne says, a parochial North-world social type, who either can be at risk or a risk in regard to others. Thus, the question remains: what does the subjection under the standardized risk model imply in regard to impact assessments in the field of data protection, privacy and surveillance? Does it mean following the same preemptive logic as it is known from other areas of risk management? And is the claim that the future present could be governed by assessing a present future needed in order to be justified as a form of subpolitics? Given its scientific appearance the notion of risk may serve to hide the fact that a power struggle always lies at the core of impact assessments, a power struggle that finds its expression in a certain tension between the knowledge that is produced and the interests that take part in the process.

The language of risk provides the framework for how knowledge is produced. The framed knowledge needs a certain quality according to the predefined purpose of the whole assessment action. To structure, inform and thus support decision-making it needs to have a certain stability. The significance of a risk, the probability of its occurrence, and the magnitude of its impact should the risk occur need to be classified in order to be able to measure and seemingly objectify the impact. As early as the 1990s Bennett and Raab recommended "a healthy skepticism" to "any attempt to construct a hard-nosed evaluation of the performance of a data-protection system"[23] and indeed not everything seems quantifiable or classifiable as for example the embarrassment of body searches and profiling, and thus other methods are needed. However, the claim may also confront arguments derived from forms of evaluation other than risk assessments. The aim is to scientifically produce evidence, to come to the most rational or scientifically legitimate conclusion.

However, to get an understanding of the tension between knowledge and power that is at stake here, we can contrast the outcome of a scientific discussion on the one hand with the outcome of a negotiation on the other. A *scientific or rational discussion* tries to produce knowledge. It confronts arguments and scientifically produced evidence and tries to come to the most rational or scientifically legitimate

[20] Wynne, Brian, Risk as globalizing 'democratic' discourse? Framing subjects and citizens, in: *Science and Citizens: Globalization and the Challenge of Engagement*, Melissa Leach, Ian Scoones and Brian Wynne (eds.) (London: Zed Books, 2005), p. 70.

[21] Wynne, Brian, Risk and Environment as Legitimatory Discourses of Technology: Reflexivity Inside Out?, *Current sociology*, 2002, 50, p. 468.

[22] Wynne, Brian, Risk as globalizing 'democratic' discourse? Framing subjects and citizens, p. 72.

[23] Bennett, Colin J., and Charles D. Raab, *The Governance of Privacy: Policy Instruments in Global Perspective*. (Aldershot: Ashgate, 2003), p. 188.

conclusion. This conclusion can change when new evidence is produced, but there is a clear idea of progress. It is the conclusion which is fits best to the evidence or rational arguments that will be considered the best solution and that will replace the earlier, and now considered faulty, conclusion.

On the other hand, when differing interests are present, there is no best solution. We get a *negotiation* which can lead to a compromise. Several compromises are possible and depend on the power of the actors around the table to influence the valuation of an impact. And a compromise is not guaranteed. The conflict may remain among the actors. Who counts as relevant actors in an assessment procedure to discern relevant facts and who does not, remains challenging, e.g., given the fact that surveillance is an inherently power-related process with the surveilling party exerting power over the surveilled party. Highly different interests may clash. However, what happens if we mix these two poles of rational discussion and of negotiation? What happens with the production of knowledge in an interest-driven context?

In the context of impact assessment knowledge and power are inextricably linked. Impact assessments produce knowledge, but are also the object or site of a struggle between interests. Trying to single out the knowledge component by making 'evidence-based' assessments and excluding mere 'political beliefs', is in practice granting a monopoly to experts and locking out broader participation. It implies excluding the public, separating technology from society and thus dismissing science, technology and society as mutual co-evolutionary, generative and open processes that entail different roles and conflicting objectives of participating actors and communities.[24] Defining what knowledge is, is in itself an element of power.

Accordingly, stakeholder participation is usually promoted as a method to ensure that a broad range of issues is raised and therefore a wide spectrum of knowledge produced in PIAs as well as in SIAs. As Wright has put it, participation allows discovering risks otherwise not considered. Ignoring these risks or refusing to assess them can lead to liability or sanctions. Stakeholder participation can also be used to assess risk perceptions, "testing the waters" when it comes to acceptance. The overall objective is thus to a make a decision and an investment more "accountable" as well as "robust" in terms of acceptance. This robustness stays weak. The results of this participation remain limited to knowledge about perceptions of stakeholders, without assuring that the concerns of stakeholders are also effectively taken into account.

In general we cannot say that in the PIA and SIA literature the political aspects are ignored, but that it is presumed that the elements of knowledge and power can be separated. This literature considers impact assessments as tools to produce knowledge, and stakeholder involvement has to be legitimized in this context. It seems a mere addition of information and scrutinizing efforts, which can be separated from the conflict of interests. Through this separation of knowledge and politics impact assessments become a tool to de-politicize the issues.

[24] Jasanoff, Sheila, *States of knowledge. The co-production of science and social order*. (London: Sage, 2004).

5.3 Between Science and Co-decision. Cashmore's Typology of Environmental Impact Assessments

These presuppositions can be questioned. In our view impact assessments are political tools and not just tools to produce knowledge. With this tool issues can be re-politicized and the political debate between stakeholders newly organized. To clarify this we present a typology of impact assessments made by Matthew Cashmore, which presents very well how decisions concerning the purpose of impact assessments and its envisaged outcome frame the role given to public participation and knowledge. This typology helps us to uncover the political aspects present in impact assessments.

Given its evolution since the 1970s, the recent literature on impact assessment in the environmental context offers a reflection on the role of science and the link between knowledge and power in impact assessments and how different accounts of this relation imply different foci. Matthew Cashmore developed a typology of five distinct models of the role of science in Environmental Impact Assessments by following two gradients, one emphasizing "science" and an opposite one emphasizing "stakeholder involvement" and "value judgements". The models are thus spread between two main paradigms, "applied science" on the one hand and "civic science" on the other.[25] The way science and knowledge are approached in these five types has an impact on the purpose of the impact assessment, on what is considered as an appropriate outcome, and consequently also on the methodologies used in undertaking an impact assessment. Purpose, envisaged outcome and the methodology are thus interrelated.

The side with the most emphasis on the scientific aspects is represented by the "analytical science model". Impact assessments of this type are part of the applied science paradigm, which draws a clear distinction between "facts" as the "pursuit of science" and "value judgements" as the "realm of decision-making". The undertaking of an EIA is similar to dealing with a research problem, and EIAs are subjected to the same procedures and practices as other scientific research, such as peer review. Statements on impacts are hypotheses which can be subjected to rigorous falsification. Factual and value judgments must be kept strictly apart.[26] The realm of knowledge is thus strictly separated from the realm of politics. Accordingly, stakeholder involvement plays no role in the assessment process, but is part of the decision-making itself.

The second model is the "environmental design model", which still belongs to the applied-science paradigm, but as the name already suggests, aims to impact the project or policy design. However, it arose from a critique of the first model, which

[25] Cashmore, Matthew, "The role of science in environmental impact assessment: process and procedures versus purpose in the development of theory." *Environmental Impact Assessment Review* 24 (2004): pp. 405–414.

[26] Ibid., pp. 408–409.

it considers too passive and reactive and consequently as leading only to end-of-the-pipe mitigation of negative impacts. In the analytical science model the impacts can only be fully tested when the project is finished and implemented, and not before. But this is seen as a scientific weakness of the EIA model. This second model accepts that scientific precision and rigor is not possible before the implementation of the project, but rather focuses on practical advice concerning design choices. The impact assessment becomes a component of project design.[27]

Although this model starts from the same epistemological position as the analytical model, it stresses planning and engineering rather than conducting scientific research. Educated stakeholders in planning, engineering and management form the basis and a very specific knowledge is needed to provide "timely, practical advice which facilitates sound design choices".[28] Knowledge and politics are thus still separated in this model. Involvement is based on technical expertise. Involvement of non-expert stakeholders, who cannot provide expertise concerning these design choices, is seen rather as an element of the broader planning process and not of the EIA itself.

The third model, the "information provision model", is still mostly analytical in its attempt to identify and evaluate a range of feasible alternative options. But it takes into account that scientific practice is limited in its capacity to research and predict accurately the consequences of a project. Instead of trying to achieve scientific rigor or certainty, it proposes using the "best practicable scientific techniques in a holistic assessment of alternatives and consequences".[29] It also accepts that value judgments are part of the planning process, but still maintains a strict separation of factual judgments.[30] Stakeholder involvement is based on the added value stakeholders can give in the production of knowledge. They are seen as a heuristic to augment the knowledge in a practical and relevant way. Stakeholder perspectives on impacts may be relevant enough to be considered in proposing further falsification tests. However, the involvement is limited to consultation. It can guide the identification of alternatives or concerns about impact in an iteration between factual input and value judgments.[31] But when societal perceptions diverge from expert opinions, these perceptions are often put aside as "incorrect, irrational or parochial".[32]

Regarding the role of science the "participation model" also works with a similar impact assessment concept as the information provision model. But it accepts qualitative predictions when quantitative predictions are not feasible. The primary aim is reasonable environmental management and not accurate and precise predictions. However, the most important difference is that it considers stakeholder

[27] Ibid., p. 410.

[28] Ibid., p. 410.

[29] Ibid., p. 411.

[30] Ibid., p. 412.

[31] Ibid., p. 412.

[32] Ibid., p. 413.

involvement as an integral part of the scientific model. The role for stakeholders goes beyond mere consultation and can result in amending the proposal during deliberation. This model includes a broad and inclusive interpretation of who is a stakeholder and goes beyond experts and directly affected local communities. It recognizes that decision-making has to be transparent and responsive and that the plurality of opinions and values in society has to be considered, if not actually integrated. The separation between facts and value judgments becomes blurred and, accordingly, an impact assessment has a broader role than just informing the decision makers. It is accepted that through EIA, stakeholders can influence the decision-making process itself.[33] The legitimation of stakeholder involvement is their interest in the issue and not just their knowledge or expertise. Involvement is therefore not only an approach to broaden the knowledge base, but amounts to negotiation about what the relevant impacts are.

Finally, the "environmental governance model" sees an EIA primarily as a political process and a decision-making tool through which stakeholders become empowered. As such, an EIA "becomes a framework for negotiation and compromise",[34] and the role of stakeholders in the planning process becomes one of co-decision. Science still has a role to play, but this model follows a constructivist notion of science. It rejects the possibility of theory-neutral observation and considers objective scientific facts as artificial constructs made by social actors.[35] Scientific statements and approaches need to gain legitimacy not only by procedure, but in the deliberation between stakeholders as well, because social meanings and interpretations of such statements are multiple and heterogeneous. Deliberation is used to determine which knowledge and scientific approach can deliver relevant results for the questions at stake.

For us the interest in this typology lies in how it exposes the political elements in impact assessments. This typology orders the models according to an decreasing emphasis on the scientific aspects, which also correlates with an increasing emphasis on stakeholder involvement. The distinction we made earlier between a scientific or rational discussion, and a negotiation between opposing interests, can be recognized in the ordering over emphasis on scientific aspects and stakeholder involvement. This typology also expresses different views on the purpose of an EIA as part of decision-making and the role accordingly given to knowledge: the production of knowledge to inform decision-making, influencing such decision-making, and co-decision-making, where knowledge is produced as building blocks in negotiation. Knowledge production in this last context remains important, because it makes more fine-grained negotiation possible. Consequentially, which knowledge is considered relevant is also negotiated.

Cashmore points to the fact that there are important differences between the purpose of an EIA as "informing, influencing or integrating with decision-making

[33] Ibid., p. 412–413.

[34] Ibid., p. 413.

[35] Ibid., p. 414.

processes"[36] and that each interpretation has implications for the type of science used in the impact assessment. Again, this shows that impact assessments are political tools. What is considered as the purpose of impact assessments in the decision-making process and the envisaged outcome, and consequentially the role of science and of stakeholder involvement, are issues which follow from implicit or explicit political decisions. To separate knowledge and value questions is also a decision for a certain type of impact assessment and a specific role it can have in decision-making processes.

Although the analytical science model is the oldest within EIAs and the models later developed based on criticism of earlier ones, all of them are still present in the literature. In practice, most EIAs follow either the analytical science model or the information provision model. The participation and environmental governance models are rarely used in practice but can be found in what is promoted as best practices in some of the literature.[37]

5.4 Competing Conceptions of Knowledge

So far we showed elements of political decision making in impact assessments as a tool. But such elements are already present in the conceptions of knowledge. Cashmore and others point to the different models of knowledge used and how it relates to the methodology of an impact assessment.[38] More traditional types of impact assessments, e.g. the information provision model in Cashmore's typology, are based on rational models of knowledge, best known in the account by Popper, presuming a unified body of knowledge which is improved incrementally. In this model stakeholder involvement is a method to improve scrutinizing and the extent of the knowledge base. Information adapts knowledge in an incremental way. It slowly augments the fit between facts and theory.

Several authors point to the role of paradigms in the sense of Kuhn in policy making. Paradigms are patterns of thought providing a general model for scientific theory and practice, or for knowledge in general. Often other terms than paradigm are used, such as frame or discourse to demonstrate how knowledge is conceptualized and that subtle differences will exist between these.[39] For example,

[36] Ibid., p. 417.

[37] Partidario, Maria Rosario and William R. Sheate, "Knowledge brokerage – potential for increased capacities and shared power in impact assessment", *Environmental Impact Assessment Review* 39 (2013): p. 27.

[38] Cashmore, Matthew, "The role of science in environmental impact assessment: process and procedures versus purpose in the development of theory.", pp. 418–420.

[39] Runhaar, Hens, and Piety Runhaar and Tammo Oegema, "Food for thought: Conditions for discourse reflection in the light of environmental assessment", *Environmental Impact Assessment Review* 30 (2010): pp. 339–346; Partidario, Maria Rosario and William R. Sheate, "Knowledge brokerage – potential for increased capacities and shared power in impact assessment", *Environmental Impact Assessment Review* 39 (2013): 26–36; Juntti, Meri, and Duncan Russel, John

Runhaar et al. (2010) use the term discourses in an empirical study of the discourses during an impact assessment on gas mining and fishing in the Dutch Waddenzee:

> Discourses refer to the ways in which (groups of) actors give meaning to particular phenomena (e.g. a particular environmental problem) and help making sense out of what is happening in the world around us. ... In this context, decision-making is conceptualised as a "system of competing discourse coalitions and their struggles to 'control shared meanings' and to gain acceptance of their framing of a policy issue" (Durning 1995) and controversies are explained by the presence of two or more conflicting discourses and associated 'discourse coalitions'.[40]

However, the main point is that following Kuhn's understanding of paradigm a different understanding of knowledge appears than within the Popperian rational model. Knowledge is in itself an agreement or consensus of a community of scientific practice and as such is also historical. Following a Kuhnian or Popperian model of knowledge (or even better, model of science) in the context of impact assessment changes the role of science, knowledge and stakeholder involvement substantially. When paradigms conflict according to the Kuhnian model there is more at stake than just an interpretation of certain facts. It is rather the whole framework of sense-making of facts which is at stake and about which there is disagreement. The conflicting paradigms become "incommensurable",[41] they lack a common standard or measure through which to assess the information. A change of paradigm forces reworking what are facts and how to make sense of them.

Disagreements between stakeholders in an impact assessment context often reflect a conflict between paradigms. Runhaar et al. look at the factors which make participants in IA reflect on their paradigms (called discourses in their account). They point to the role of these discourses as filters of information and the slow acceptance of the need to review them due to contradictory information. People have the tendency to favor information that confirms their beliefs, and in this account also their interests. Discourses are not just ways to make sense of a range of scientific observations, but are also ways to legitimize and rationalize interests. Interests, values and facts are linked and rationalized into one paradigm, through which new information is assessed.

Again, political elements are an inherent part of the process through which knowledge is produced. In order to come to a common understanding on impacts, the different actors also have to establish a common discourse through which facts and values are evaluated. That means that in order to come to an agreement, the

Turnpenny, "Evidence, politics and power in public policy for the environment", *Environmental Science & Policy* 12 (2009): pp. 207–215; Cashmore, Matthew et al., "Evaluating the effectiveness of impact assessment instruments: Theorising the nature and implications of their political constitution", *Environmental Impact Assessment Review* 30 (2010): pp. 371–379.

[40] Runhaar, Hens, and Piety Runhaar and Tammo Oegema, "Food for thought: Conditions for discourse reflection in the light of environmental assessment", *Environmental Impact Assessment Review* 30 (2010): p. 340.

[41] Kuhn, Thomas, *The structure of scientific revolutions*. (Chicago: University of Chicago Press, 2012), p. 149.

different actors have to reflect on their incommensurable discourses. Such reflection is not just a question of evaluating information, because the yardsticks through which the actors evaluate are incommensurable. Runhaar et al. point to elements such as trust and the role of a mediator in the assessment process as important in order to achieve such common discourse or evaluation yardsticks.[42] These are elements normally not considered to be part of a scientific method, but which are more common in a political context such as negotiations. But producing a common discourse implies a negotiation between incommensurable discourses. And this even more so, because the way actors perceived factual information proved to be dependent on their interests at stake. Negotiating common discourses for the evaluation of factual information could not be separated from negotiating common discourses for the interests at stake.

Also Partidario and Sheate (2013) take a constructivist turn and explore the relevance of knowledge brokerage which can be understood as negotiating knowledge.[43] Knowledge brokerage is understood as a mechanism to transfer research evidence into policy and practice. They point to a shift in the understanding of impact assessments from knowledge production for informing policy debates to learning and the collective production of knowledge. There they highlight the importance of political elements as trust and power sharing. It might sound strange from the point of view of the rational model of knowledge to take such political elements into the realm of knowledge production. But the observation that in a risk society knowledge must increasingly legitimate itself implies the confrontation between conflicting discourses or paradigms. Producing a common paradigm – a common framework to evaluate factual knowledge – in this context also implies negotiation between actors with different interests at stake.

What the purpose is of impact assessment and of stakeholder participation depends heavily on the knowledge model followed. Using such a paradigm model of knowledge allows a different understanding of the role of stakeholder participation. In this model of knowledge the actors negotiate what knowledge is relevant, how it is produced, etc. When on the contrary the rational model of knowledge is used, the role of stakeholder participation is limited and it remains highly questionable if the public is actually participating.

The rational model frames knowledge in order to support political decision-making outside of or following the assessment. The paradigm model, emphasizing power struggles instead, allows including decision-making into the assessment itself. Thus both knowledge models imply and create a different decision-making mechanism, and they even follow a different decision theory. While the first separates it from the assessment and offers rather an understanding of decision-making

[42] Runhaar, Hens, and Piety Runhaar and Tammo Oegema, “Food for thought: Conditions for discourse reflection in the light of environmental assessment”, pp. 344–345.

[43] Partidario, Maria Rosario and William R. Sheate, “Knowledge brokerage – potential for increased capacities and shared power in impact assessment”, *Environmental Impact Assessment Review* 39 (2013): 26–36.

referring to the monopoly of science, the latter includes it into the assessment and follows a democratic model of decision-making referring to a demonopolisation of scientific truth.

5.5 Interdisciplinary Cooperation Within Impact Assessments

If knowledge production is linked to power and this linkage again determines how decisions are made, then the framing as well as the negotiating will not only be of importance between stakeholders of obviously different interests – such as between representatives of the security industry on the one hand and privacy advocates on the other – but also within certain groups involved in the assessment. Security professionals, for instance, are a less homogeneous group than is usually thought. There are different views on the meaning of security and it will depend on the respective professional role what criteria are actually seen as relevant in order to describe in concrete terms what is really meant by security. A case study on the introduction of a security measure at a German airport has shown how problems can pop up at a later – and possibly more costly – stage, when meanings are not considered in advance.[44]

In the same way, the integration of different disciplinary perspectives involved in an impact assessment is confronted with the need to negotiate respective models of knowledge and scientific practice. And again, discrepancies between the disciplines demonstrate that different conceptions are in place, as for example a legal and a sociological one, which both have a certain claim in impact assessment. Both perspectives have their method of selecting relevant persons and relevant practice, and their method to establish facts about them. Both also differ widely in their ways of selecting and assembling. Both perspectives appear at first sight to be in different worlds. Assessments inspired by sociology may insist on the perceptions, struggles and micro-politics within and beyond certain contexts. A legal approach is oriented to come to normative decisions and sieves out what is relevant according to its legal concepts and norms, while making an abstraction of everything else. A certain ambiguity over what is really at issue will stay. And indeed, whatever scientific approach is followed may provoke different expectations and may also be seen as indicative of certain interests of those who have initiated the assessment in the first place.

As a point of departure we may look at the proposal for a legal obligation to perform a Data Protection Impact Assessment (DPIA). If considered as a mere compliance check, it is reduced to a legal instrument. According to a certain

[44] For an account see: Hempel, Leon and Lars Ostermeier, Tobias Schaaf, DagnyVedder, Towards a Social Impact Assessment of Security Technologies. A bottom-up approach. *Science and Public Policy* (2013) 40 (6): pp. 740–754.

normative catalogue of existing principles its conformity is either approved or disapproved. What is beyond, stays out of the sight, the interest and also the responsibility of the respective lawyer. Thus, compliance checks are not checks on all potential consequences. It is limited to the potential legal consequences while disregarding impacts not recognized by law as relevant. The objective of this exercise is, however, to place decision makers in a position where they can effectively make a decision by reducing the complexity as much as possible. Knowledge about the issue is consulted accordingly and scientific insights subjected to that predefined end. The role of other sciences – whether natural or social sciences – is reduced to producing some kind of external evidence. This is as reductionistic as the limitation of EIA to natural science research on environmental impacts.

However, the implicit scientific hierarchy of compliance checks is less an issue of the legal approach as such, but is rather due to limited understanding of both law and impact assessments. First, it ignores that impact assessments are political instruments which cannot be reduced to a purely legal exercise. Law has a role to play but is not the only relevant viewpoint through which impacts can be discerned. Second, given the complexity of socio-technical systems today it remains impossible to follow such a causality program as compliance checks do. The agenda of an impact assessment does not have to be limited to strict legal compliance, nor does the legal approach have to be limited to checking legal compliance. E.g. human rights law can be used to systematically evaluate impacts on freedoms, legal or not. In this approach we look at which freedoms are protected by human rights law and look at how technology has an impact on these freedoms.[45] In this case it also helps to establish impacts which are not problematic from a legal viewpoint but are still relevant for other concerns. For instance, an impact on a freedom which is considered legal can still be considered annoying by a traveller and therefore minimizing it can be important in order to improve acceptance. Law has many uses and users, of which the legal practice of judges is an important one, but which coexists with that of regulators, politicians, etc.

The challenge is to make the complexity of socio-technical systems a reference point for impact assessments today. Impact assessments in the area of data protection, privacy and surveillance require an interdisciplinary cooperation for obvious reasons. The developments at stake are too complex to follow one single approach. To develop a methodology for an impact assessment thus remains a challenge as it necessarily implies an assemblage of different practices to discern and evaluate impacts. Within such cooperation each discipline has its terminology and practice of assembling relevant facts and relations. These can be quite different and can lead to misunderstanding especially when the same or similar terminology is used with completely different meanings.

[45] This approach was used in WP4 and 8 of the SIAM-project. See D 4.7 and D 8.2., see: http://www.siam-project.eu

Impact assessments are sites of negotiation between different disciplinary practices. Law establishes what are legally relevant subjects (e.g. data subject, data processor), objects (e.g. personal data), relations between those or actions on each other (e.g. what is processing of personal data, what is interference with a human right) and when these are legal or in violation of the legal framework (e.g. what is legitimate processing of personal data, what is a violation of a right). For the interpretation of these terms and to establish their precise meaning legal practitioners draw on jurisprudence, which reflects a body of legal practice and knowledge on how to deal with such situations. In this body of legal practice a wide range of cases is present. In the case at hand legal practitioners try to make an application of legal norms, coherent with the wider body of legal norms and principles and with the past practice accumulated in the jurisprudence. Considering legal norms implies considering each thinkable case. Thus as a practice the law entails and is always inherently confronted with contingency - with what is possible but not necessarily given.

In this respect the agenda of the social science correlates with that of the legal science. It aims at integrating as many alternatives as possible, claiming that the empirical reality of a case is always somehow more multi-variant than can ever be assessed. For instance, ethnographical approaches aim to differentiate how situations are framed in order to create sense and to interact in critical and insecure situations. As such these frames are dependent upon various elements. However, each new frame means a further differentiation of a possible case and thus a further prolongation of a decision to be made. The complexity as such thus increases steadily and there is hardly any closure of the learning of the social world as such.

Thus, both the legal scholar and the social scientist hesitate in regard to their decisions, both have their normative elements in regard to what is selected as a relevant issue, who is a legitimate source and so on. Both thus have their empirical elements and their answers to how a fact is established as being either social or legal. The social science can provide additional differentiations and possibilities to increase the law's selectivity. However, it cannot do this as law as Niklas Luhmann points out.[46] While the law defines what a valid element of the law is, the social and all sciences in general define what a scientifically valid observation or statement is. However, a valid statement for one discipline is at most an external fact in the other. Luhmann points to the facts that each science or discipline as law contains its own mechanism of closure through which it reduces complexity and creates its own identity.[47] That means its own mechanism to recognize something as an element of its discipline.

[46] On the specific role of sociology in relation to law, see: Luhmann, Niklas, Ausdifferenzierung des Rechts. Beiträge zur Rechtssoziologie und Rechtstheorie. (Frankfurt am Main, Suhrkamp 1999), p. 259. See also Luhmann, Niklas, *Law as a social System*, (Oxford: Oxford University Press 2004), p. 85.

[47] Luhmann, Niklas, *Law as a social System*, pp. 113–117.

When we use law, sociology or a natural science in an impact assessment, they are external sources in a distinct political practice. In this practice it will be defined what is part of that practice, in other words how legal and sociological methodologies can be used to establish impacts relevant in the impact assessment and in the decision-making process in which it functions. As we saw earlier with the impact assessment typology of Cashmore, this definition, mechanism of closure in Luhmanian terms or way of assembling in Latourian terms, is not strictly defined but is established in a negotiation. The challenge with the integration of perspectives is to avoid turning them into a hierarchy with one dominant perspective and the second as auxiliary, and to make sure that both perspectives inform the assessment methodology and complement each other.

5.6 Conclusions

Impact assessments are part of the decentralization of politics. They do not stand alone as tools to produce knowledge, but above all as tools to structure a political debate between stakeholders on the impact of an envisaged project. In these tools knowledge and power are inextricable, or rather the place and shape of science and knowledge in impact assessments follows from political decisions about its purpose and role in the decision-making process. This placement of science also determines the rationale and shape of stakeholder involvement. Impacts are not value-free notions but stand for impacts on recognized interests. As such, impact assessments are also derived in negotiations, and the knowledge produced on impacts is negotiated knowledge.

The literature concerning PIA, DPIA, security and surveillance impact assessment has limited itself till now mostly to procedural issues, but has given little attention to the envisaged outcome of an impact assessment and its role in the decision-making process. The discussion on these new forms of impact assessment has to take the experience and lessons learned with EIA into account and include in its theorization considerations on substantive outcomes and purpose, or more broadly on impact assessments as political tools. The explicit reflection on how and which knowledge gets produced in an interest-driven context can help to improve the development of practical models of, and methodologies for, impact assessments, which are more than just the ritual fulfilling of a regulatory requirement.

Awareness of the political nature of impact assessments and the negotiated character of the knowledge produced can also help to approach the problem of integrating various sciences or disciplines. The relation between different disciplines in an impact assessment is not fixed. And using one dominant perspective while using other disciplines as auxiliary leads to a myopic, limited view and a reduction of the impact assessment to a legal or a research exercise. In the end an impact assessment is a political process and has its own mechanism of closure through which a definition is made as to what a relevant impact and relevant knowledge about them is. This closure mechanism is created from outside by defining the purpose and envisaged outcome of the impact assessment in the decision-making process, and from within by the power positions of the stakeholders and the space left for negotiation among them.

References

Alonso, Sonia et al., *The Future of Representative Democracy*, (Cambridge: Cambridge University Press 2011)

Beck, Ulrich. *Risk Society. Towards a New Modernity.* London: Sage Publications, 1992

Bennett, Colin J. and Charles D. Raab, *The Governance of Privacy: Policy Instruments in Global Perspective.* Aldershot: Ashgate, 2003

Cashmore, Matthew. "The role of science in environmental impact assessment: process and procedures versus purpose in the development of theory." *Environmental Impact Assessment Review* 24 (2004): 403–426

Cashmore, Matthew, Tim Richardson, Tuija Hilding-Ryedvik, Lars Emmelin, "Evaluating the effectiveness of impact assessment instruments: Theorising the nature and implications of their political constitution", *Environmental Impact Assessment Review* 30 (2010): 371–379

Guston, David H. and Daniel Sarewitz, Real-time technology assessment. *Technology in Society* 24 (2002): pp. 93–109.

Holzer, B. and Mads P. Sorensen, Rethinking Subpolitics. Beyond the 'Iron Cage' of Modern Politics? Theory, *Culture & Society* April 2003 vol. 20 no. 2 79–102.

Jasanoff, Sheila, *States of knowledge. The co-production of science and social order*. (London: Sage, 2004)

Juntti, Meri, Duncan Russel and John Turnpenny, "Evidence, politics and power in public policy for the environment", *Environmental Science & Policy* 12 (2009): 207–215

Kuhn, Thomas, *The structure of scientific revolutions.* Chicago: University of Chicago Press, 2012.

Latour, Bruno *We Have Never Been Modern*, (Cambridge: Harvard University Press 1993)

Latour, Bruno, *Pandora's hope, essays on the reality of science studies*. (Cambridge: Harvard University Press 1999)

Latour, Bruno, *The Making of Law. An Ethnography of the Conseil D'Etat*, (Cambridge: Polity Press 2010)

Hempel, Leon and Lars Ostermeier, Tobias Schaaf, Dagny Vedder, Towards a Social Impact Assessment of Security Technologies. A bottom-up approach. *Science and Public Policy* (2013) 40 (6): pp. 740–754.

Luhmann, Niklas, Ausdifferenzierung des Rechts. Beiträge zur Rechtssoziologie und Rechtstheorie. (Frankfurt am Main, Suhrkamp 1999.)

Luhmann, Niklas, *Law as a social System*, (Oxford: Oxford University Press 2004)

Macnaghten, Phil, Matthew B. Kearnes and Brian Wynne, Nanotechnology, Governance, and Public Deliberation: What Role for the Social Sciences? *Science Communication* 27 (2005): pp. 268–291.

Mathiesen, Thomas, Lex Vigilatoria – Towards a control system without a state? in: Deflem, Mathew (ed.) *Surveillance and Governance: Crime Control and Beyond,* Bingley, Emerald Group Publishing Limited, pp. 101–130.

Michaelsen, Danny, Franz Walter, *UnpolitischeDemokratie. ZurKrise der Repräsentation*, (Berlin: Suhrkamp 2013)

Partidario, Maria Rosario and William R. Sheate, "Knowledge brokerage – potential for increased capacities and shared power in impact assessment", *Environmental Impact Assessment Review* 39 (2013): pp. 26–36

Prainsack, Barbara and Lars Ostermeier, *Report on methodologies relevant to the assessment of societal impacts of security research*, D 1.2 Assert-project

Runhaar, Hens, Piety Runhaar and Tammo Oegema, “Food for thought: Conditions for discourse reflection in the light of environmental assessment”, *Environmental Impact Assessment Review* 30 (2010): pp. 339–346

Schot, Johan and Arie Rip 1997, The Past and Future of Constructive Technology Assessment. *Technological Forecasting and Social Change* 54 (2–3): pp. 251–268.

Spiekermann, Sarah, The RFID PIA – developed by industry, agreed by regulators, in: David Wright and Paul De Hert (eds), *Privacy Impact Assessment*, (Dordrecht Heidelberg London New York: Springer, 2012), pp. 323–346

Vanclay, Frank, “International principles for social impact assessment”, *Impact Assessment and Project Appraisal*, Vol. 21, No. 5, 2003, pp. 5–11.

Williams, Robin 2006, Compressed Foresight and Narrative Bias: Pitfalls in Assessing High Technology Futures. *Science as Culture* 15 (2006): pp. 327–348.

Wright, David and Paul De Hert (eds), *Privacy Impact Assessment*. Dordrecht Heidelberg London New York: Springer, 2012

Wright, David and Charles D. Raab, “Constructing a surveillance impact assessment”, *Computer Law & Security Review* 28 (2012): 613–626

Wright, David, “The state of the art in privacy impact assessment”, *Computer Law & Security Review* 28 (2012): 54–61

Wright, David, and Kush Wadhwa, *A step-by-step guide to privacy impact assessment. Empirical research on contextual factors affecting the introduction of PIA frameworks in EU Member States*, Poland, April 2012. Available at: http://www.piafproject.eu/ref/A_step-by-step_guide.pdf.

Wynne, Brian, “Risk as globalizing ‘democratic’ discourse? Framing subjects and citizens” in *Science and Citizens: Globalization and the Challenge of Engagement*, edited by Melissa Leach, Ian Scoones and Brian Wynne, 66–82. London: Zed Books, 2005.

Wynne, Brian, Risk and Environment as Legitimatory Discourses of Technology: Reflexivity Inside Out?, *Current sociology*, 50 (2002): 459–477

Chapter 6
Data Processing in Employment Relations; Impacts of the European General Data Protection Regulation Focusing on the Data Protection Officer at the Worksite

Clara Fritsch

Abstract From the 1990s European Unions are increasingly confronted with ignored employees' privacy or misused employees' personal data. There has been a vivid European discourse about this issue in the early 2000s. The European GDPR brings the topic back to the European agenda. The article points out who is involved in employee data protection from side of the employees' interest organizations. The contribution further describes which are the employees' interests stressing some crucial points of the GDPR such as the data protection officer at company site and the article on data protection in employment relations. The author tries to figure out how the GDPR matches the employees interests – or otherwise. Therefore she compares the European Commission's approach with that of the LIBE-committee to see which one would serve more the employees' fundamental right to privacy.

This article gives an insight on how the European Data Protection Regulation (EDPR) will effect labour relations and looks for consideration of employees' interests within the EDPR. According to Harding,[1] Haraway,[2] and other representatives of the "standpoint theory", it is important to openly state the position of the author. I am a sociologist, working with the Austrian Union of Private Sector Employees, Graphical Workers and Journalists (GPA-djp). My main field of work is consultation of works councils who are responsible for privacy issues at the

[1] Hirsh Elizabeth and Garry A. Olson, "Starting from Marginalized Lives: A Conversation with Sandra Harding", JAC, journal of Rhetoric, Culture, & Politics (1995).

[2] Haraway Donna, "Situated Knowledges: The Science Question in Feminism and the Privilege of Partial Perspective" Feminist Studies (1988, Vol 14, No. 3).

C. Fritsch (✉)
Union of Private Sector Employees, Graphical Workers and Journalists, Alfred Dallinger Platz 1,
A- 1034 Vienna, Austria
e-mail: clara.fritsch@gpa-djp.at

S. Gutwirth et al. (eds.), *Reforming European Data Protection Law*,
Law, Governance and Technology Series 20, DOI 10.1007/978-94-017-9385-8_6

workplace, employees' data protection and monitoring systems. Dealing daily with privacy issues at workplaces – whether it is a newly installed surveillance camera, an international mother-company's request to receive all employees' performance data, a whistle-blowing hotline necessary according to the US-American Sarbanes-Oxley Act or a new navigation device placed in all company cars without the approval of employees or workplace representatives – is the very practical background of this text. Workplace experience shaped this article on one hand. On the other hand, I was involved in law amendments that deal with workers privacy – both in Austria and Brussels. My task was to promote the employees' view and interests in discussions with politicians at the European Trade Union Confederation (ETUC), with members of the European Parliament and with Representatives of the European Commission. These discussions are another background shaping this text.

Employees' interests nowadays are losing weight all over Europe (Busch et al. 2012).[3] Their rights are cut and social exclusion is on the rise. Thus, they are marginalised – especially since the economic crisis. The standpoint methodology postulates that research should initially concentrate on marginalised groups. The perspective of the "marginalised lives" is inevitable for science, as Sandra Harding[4] says.

The epistemological approach of this text is Karin Knorr-Cetinas[5] *Manufacture of Knowledge* where she shows that scientific work always depends on social (and technical) means and interaction. New scientific texts are always shaped by several different players. I tried to demonstrate – following the conventions of Knorr-Cetina – how different players shape a new European law.

Empirically the article mainly uses diverse writings by Austrian and international unions and other organisations focusing on the impact the EDPR will have on employees' interests.

The aim of the contribution is to link practical experience with the academic sphere by expressing the standpoint of marginalised employees' interests in the field of privacy politics at workplaces.

6.1 An Outline of Employee Data Protection

All over Europe the use of personal data of employees is business. Personnel administration by personal information systems, personal data created by the use of email and the internet, data of working time records, attendance and sickness records, data from video cameras, and many more information and communication

[3] Busch Klaus et al., "Eurokrise, Austeritätspolitik und das Europäische Sozialmodell, Wie die Krisenpolitik in Südeuropa die soziale Dimension der EU bedroht" (2012).

[4] Harding Sandra, "Standpoint methodologies and epistemologies: a logic of scientific inquiry for people", in UNESCO and International Social Science Council (2010).

[5] Knorr-Cetina Karin, *Manufacture of Knowledge* (Oxford 1981).

technologies (ICT) are implemented on company levels generating and administrating personnel data. Employers all over Europe and beyond precede much more data than is effectively needed to fulfill legal or contractual requirements.

Sure, data protection is a topic concerning everyone but employees as data subjects often are double victims once as citizens and consumers and secondly as dependent workers. Sometimes being an employee and a private person concerned is so closely connected (for example, when working at a hospital and having personal medical records stored at the same place or when working at a banking institution and being forced to have a banking account there as well) it leads to misuse of personal data. Looking at dynamic data, connection data or just log files, one can easily recognize that personal data is sometimes created automatically, without consent or even knowledge of the data subject, indicating that employees' access and the right to information is difficult to achieve. The information imbalance is evident. Employers might use this data without informing the employee – the result may be a surprising end of the employment relation.

Throughout history working conditions changed with tools and instruments of work. The biggest change until now was the industrial revolution turning hand work in machines' work. Currently we are facing a digital revolution shaping nearly every workplace.[6] ICT has changed working conditions in terms of reaction time, multitasking, availability of knowledge and – foremost important in matters of fundamental rights – monitoring possibilities. Systems are much more interdependent and linked to each other than they were in the twentieth century. Unified communication systems, shared documents and cloud services transform employees into anywhere- and anytime-workers, who at the same time can be easily traced and tracked. Acquisition and retention of employees' personal data by ICT is happening at high speed nowadays. The large and further increasing number of data leads to the use of information without caring about the data processing principles set by the European Commission in the European Data Protection Directive regarding finality, proportionality, transparency – just to mention the most important ones.

6.2 European Scientific Research on Employee Data Protection

EU-wide comparisons concerning individual awareness on data protection at the workplace among employees in general and among employees responsible for ICT are evidence of highly differing consciousness within the EU countries. An average of every third employee in the EU feels well informed about his/her data protection rights and just half of the employees trust their employers.[7] Just 13 % of the 4.800

[6] European Commission, *The European e-Business Report, A portrait of e-business in 10 sectors of the EU economy, 5th Synthesis Report of the e-Business W@tch* (Brussels, 2006).

[7] European Commission, *Special Eurobarometer Data Protection* (Brussels, 2003).

data controllers interviewed in 27 EU member states are familiar with the national data protection law and the same amount frequently contacts the national data protection authority.[8] These few figures reveal the necessity of a data protection officer at the worksite (DPO) in order to fulfil the legal requirements and to protect the employees' fundamental right to privacy. DPOs can strengthen employees' privacy at the workplace since they make sure that the company's data proceedings correspond with data protection law and other law applicable to the line of business. According to the Austrian Private Sector Union DPOs should be the information link between employer, employees, clients, customers and business partners. Currently Germany is the only country within the European Union that has implemented a mandatory DPO at company level for companies with more than nine employees dealing with data proceedings.

Following the European Data Protection Directive each member state shall implement the directive into national law, hence should have an equivalent data protection level. But this is not the case in the employment context, as some few studies have shown dealing with national legal frameworks as well as industrial relations. Available studies on an international level are missing some crucial points. Some authors deal with an international scope, but do not focus on labour law,[9] other findings are limited to the comparison of legal standards regarding the use of email and the internet at the workplace, but do not include other data processing.[10] The European Article 29 Data Protection Working Party conducted a summary of the national legislation on surveillance and monitoring of electronic communication in the workplace in 2002, describing that the then member states were missing other data processing as well.[11] None of these studies combines the legal situation with technical innovation at workplaces and the only one that does[12] has no neutral approach to technology. None of these studies includes the member states that joined the European Union after 2004. It seems as if the discourse had its peak in the early years of the 2nd millennium. A more recent study was published in 2011, but it is limited to the Australian law and to the use of Email and internet.[13]

This might be caused by the fact, that there are diverse legal backgrounds as well as diverse cultures in data protection in general. The "Eurobarometer" 2008 detected

[8] European Commission, *Flash Eurobarometer Data Protection in the European Union Citizens' perceptions* (Brussels, 2008).

[9] Lilian Mitrou and Maria Karyda, *Employees' privacy vs. employers' security, Can they be balanced?* (Elsevire Ltd. 2005).

[10] Catherine Delbar et al., "New technology and respect for privacy at the workplace," *European Industrial Relations Observatory* (2003).

[11] Article 29 – Data Protection Working Party, *Working document on the surveillance of electronic communications in the workplace* (Brussels, 2002).

[12] Catherine Delbar et al., "New technology and respect for privacy at the workplace", *European Industrial Relations Observatory* (2003).

[13] Anne O'Rourke, Julian Teicher and Amanda Pyman, "Internet and Email Monitoring in the Workplace: Time for an Alternate Approach", *Journal of Industrial Relations* (2011 vol. 53).

that 72 % of the EU citizens do not even know about their national data protection authority, whose purpose is – amongst others – to protect individuals against data misuse. In 2010, the European Union Agency for Fundamental Rights realised a study dealing with the role of national data protection authorities. Findings are that these authorities are organised quite differently regarding their independency, resources, assertiveness and sanction possibilities.

6.3 Legal Situation

In the last 15 years there have been several attempts to regulate privacy at workplaces constraining the use of monitoring and surveillance within employment relationships respectively. Some European countries have specific legislation in this area. In 2004, Finland amended the "Act on the Protection of Privacy in Working Life" based on an act first passed in 2001. This is the most elaborated act on this topic in the European Union specifically dealing with employee data proceeding and including applicants data as well. Of course, jurisdiction and single clauses within labour or constitutional law deal with workplace monitoring, workplace privacy and workers representatives' participation, but single acts of legislation on this very topic are a rare good.

Intersectoral collective agreements in Norway, for example, state that privacy at workplaces is to be retained. The Belgian national collective agreement No. 81 from 2002, the "agreement on the protection of the private lives of employees with respect to controls on electronic on-line communications data", is another European "early bird" regulating data protection within industrial relations. However, it only applies to private employment relations. The agreement states the goals allowing for the online monitoring of employees' behavior at the workplace, e.g. technical functioning of the ICT as well as controlling of inner company internet compliance.[14]

The problem with compliance guidelines is that employees or workplace representatives are never involved when such compliance regulations, behavior guidelines, codes of conduct Binding Corporate Rules (BCR) – or however the documents are called – are established. Putting surveillance measures in force in order to control employees' behavior according to employer-driven compliance always puts the employee on the weaker part. Compared to the set of possibilities within the GDPR enabling an employer to process employees' personnel data, an increasing importance of Binding Corporate Rules (BCR) can be indicated.

Back to the Belgian national agreement, we can see an advantage for Belgian employees. Individual controlling measures must always be preceded by generic controlling measures. Hence, employees are better protected against false suspicions and probably consequently caused dismissal. Furthermore, Belgian employers must

[14] Catherine Delbar et al., "New technology and respect for privacy at the workplace", *European Industrial Relations Observatory* (2003).

inform employees and their representatives prior to any monitoring measures. The approach of generic before individual monitoring also follows the Portuguese data protection authority that published guidance on employees' internet and email use.

Many national data protection authorities elaborate guidelines and similar documents as well (for example the United Kingdom, Ireland, Italy, Austria or France) in order to deal with the data protection responsibilities within employment relations. Some national data protection authorities expressed opinions dealing especially with electronic communication at workplaces, for example, Denmark, Germany, Ireland, Italy, France or Belgium.[15] But these documents are of rather weak legal binding. Obviously, authorities all over Europe have – more or less successfully – tried to fill a legal gap.

Information duties before conducting individual surveillance measures within employment relations can be found in France, the Netherlands, Spain, Sweden or Austria. Consent of employees is explicitly needed in some national labour laws such as labour legislation in the Netherlands, France, Germany or Austria. Workplace related regulation of video surveillance exists in Belgium and Denmark.

Delbar et al. say: "Despite a lack of specific legislation, the general legal framework and principles are interpreted as having implications for employees' internet and e-mail use in some countries." The German way of getting along with employee data protection is constitutional law stipulating the right to "informational self-determination". Much adjudication are operationalizing the constitution and therefore giving guidance for workers' data protection as well. But jurisdiction differs a lot all over Europe as, for example, in Italy the employer got the right to see an employees' private email sent to the companies address anytime, while Dutch and French courts deny this recurring due to the fundamental right of keeping correspondence secret. Moreover, national jurisdiction is a weak instrument when European wide legal security shall be the outcome.

"Given the general absence of specific legislation on employees' privacy at the workplace, the introduction of such provisions has been discussed or proposed in a number of countries, sometimes with direct relevance to internet/e-mail use." state Delbar et al.[16] Finland, Germany, Norway and Sweden have tried to change this status quo and worked on specific legal acts – some of them still struggling for a better legislation on employee data protection.

[15] Hendrickx Frank, *Protection of workers' personal data in the European Union* (Leuven/Tilburg, 2002).

[16] Catherine Delbar et al., "New technology and respect for privacy at the workplace," European Industrial Relations Observatory (2003).

6.3.1 The Austrian Example

Austria is a typical example for the international legal situation. No special rules on workplace privacy, only little evidence of jurisdiction and an only slowly rising awareness of the importance of the topic shape the field of Austrian employee data protection.

Doubtless there is an economic dependency of employees on their employers. Since no employee wants to accuse his/her employer of data abuse during an existing employment contract, court rulings on the right of data protection of employees are rare. Even more so, since evidence is sometimes hard to proof. The result is no jurisdiction in Austria regarding data protection legislation. This is also driven by the fact that data protection law belongs to individual right, which means employees have to lodge an appeal before a court of first instance and pay a lawyer on their own. Workers representatives have no right to be party in the proceeding. Rulings concerning employee data protection after an employee has been dismissed refer to labour law, where more jurisdictions exist that judges can rely on. The result is a prevailing lack of data protection jurisdiction in employment relations causing legal insecurity.

A recently concluded study by an employees' interest organization (the Chamber of Labour Vienna) found, that only one out of four ICT systems that would need compulsory regulation by a works agreement, concluded between the workforce representative and the employer, is actually regulated.[17] One reason is that ICT is difficult to understand for workplace representatives as well as employers. To regulate ICT, negotiators must have at least some technical understanding and know how personnel data is proceeded. Due to the fast advance of ICT, weekly updates and new implemented systems every year, it is difficult to make up leeway. The increasing quantity of systems, some of which are corresponding with each other, neither makes things easier. Therefore, even interested employees and works councils lose track. Data protection officers (DPO) at company level could remediate this obstacle. Representative figures in Austria show that the employees are better informed and more works agreements are concluded in companies, in which DPOs have been established voluntarily.[18]

Some legislation parties in Austria are engaged in developing a legal regulation on employee data protection since 2010, but did not succeed yet. In the last 5 years, there have been several efforts to strengthen workplace privacy by legally implementing a DPO at the company level. The first attempt in summer 2010 should have brought about an obligatory DPO with dismissal protection, a 4-year working period, technical resources and knowledge as well as permanent further education.

[17] Riesenecker-Caba, Thomas and Alfons Bauernfeind, *Verwendung personenbezogener Daten und Grenzen betrieblicher Mitbestimmung: Datenschutz in der Arbeitswelt* (Arbeiterkammer Wien, 2011), 73–78.

[18] Fritsch, Clara, "Vogelstraußpolitik, der Tenor von Umfragen zum innerbetrieblichen Datenschutz in Österreich," *Arbeit und Wirtschaft* (2008): 17.

He/she should not have been bounded by employer's instructions. The position of a company DPO as the Austrian Trade Union Federation ("Österreichischer Gewerkschaftsbund", ÖGB) wanted it, should have even more weight, as he/she would only be put in place with the approval of workplace representatives and should be responsible not only for company and customer data, but also for employee personal data. The employer's interest organizations', the Chamber of Business, argument is that this would be too expensive and that there would be no necessity of such a position due to a well-functioning Austrian data protection law.

After another unsuccessful attempt to implement an obligatory DPO to the Austrian data protection law in summer 2011, the third attempt followed in 2012. This amendment was stipulating that a voluntary DPO should be implemented at company level. Again, the Chamber of Commerce did not agree and the government dropped the plan again.

6.4 Employee Data Protection by Relevant European Players

6.4.1 The European Commission

In August 2001, the European Commission started a first round of formal consultation with social partner raising the question, whether protection of employees' data requires special guidelines and if yes, how these guidelines should be expressed – by a directive, a recommendation or just a code of conduct? Employer organisations mostly found the existing legal framework sufficient and warned about excessive regulations and burdens for small- and middle-sized companies. (These concerns were expressed repeatedly when it came to consultations in 2010 as described in Sect. 6.5.2.). Unions all over Europe painted a controversial picture, stating that the existing directive is helpful but not sufficient and demanded a specific directive on workplace data protection.

In October 2002, the European Commission launched a second consultation of European social partners. In the end, the Commission elaborated a framework proposal for employee data protection including, among other details, obligatory employees' representatives' consultation before implementing new ICT, monitoring only if national data protection authorities controlled the ICT in advance and the interdiction of secret monitoring if there is no concrete suspect of a grave criminal misbehaviour.[19] (Reading the proposals made by the European Parliament's Committee on Employment and Social Affairs (EMPL) in 2013,[20] one can find some of these points again.)

[19] European Commission, *Second stage consultation of social partners on the protection of workers' personal data* (Brussels, 2002).

[20] Committee on Employment and Social Affairs, *Opinion for the Committee on Civil Liberties, Justice and Home Affairs on the proposal for General Data Protection Regulation* (Brussels, 2013).

There followed no further action from the Commission's side for a long period and the social partners did not take up the matter themselves. It was the year 2010 when the Commission started a new consultation; this time open to the public and dealing with data protection in general not specifically with employees' data protection. 288 contributions were counted when the public consultation closed. Replies were manifold as the list of contributors shows.[21]

Big players in the field of ICT (such as eBay, Alcatel, Yahoo, Vodafone or Microsoft) sent their contributions as well as public authorities and interest organisation. The latter comprising much more employer organisations from the finance, medical and ICT sector than employees' interest organisations. Papers raising awareness on the employees' special interests in data protection just came from Germany and Austria. The ETUC and UNI Global Union, the international federation of the service sector unions, also responded to the Commission's consultation.[22] National unions in the EU and their umbrella organisations seemed not to be interested in the matter at that time, while those branches whose vital interest are affected by data processing were much aware of the imminent "dangers" of a new European data protection regime.

6.4.2 The European Article 29 Data Protection Group

The Article 29 Data Protection Working Party, an assembly of all national data protection authorities including representatives of the European Data Protection Supervisor and of the European Council with the aim to interpret the Data Protection Directive from 1995 according to specific problems raising all over Europe (for example, the proceeding of geo-data, cloud computing or face recognition), published the "Opinion on the Processing of Personal Data in the Employment Context" in 2001 aiming for: "further guidance on the issues where the application of general principles of data protection raises particular problems relevant to the employment context, such as the surveillance and monitoring at the working place, employee evaluation data and others."[23] This opinion was a landmark for advocates of an individual employee data protection act. Although some efforts have been taken to come to such an international legal norm, it has not yet been concluded.

The opinion of the Article 29 Data Protection Working Party are in general very helpful for unions, as they very often outline concrete suggestions on how to deal

[21] European Commission, *Summary to the Replies to the Public Consultation About the Future Legal Framework for Protecting Personal Data* (Brussels, 2010).

[22] European Trade Union Confederation, *ETUC response to the Communication from the Commission 'A comprehensive approach on personal data protection in the European Union'* (Brussels, 2011) and Uni global union, *Submission to the European Commission communication A comprehensive approach on personal data protection in the European Union* (Brussels, 2011).

[23] Article 29 Working Party, *Opinion on the Processing of Personal Data in the employment (Brussels, 2014).*

with actual problems occurring in the working area – for example, if employees' data is transferred to non-European Union member states for reasons of bonus compensation, if external workers are located, if video surveillance is installed, and so on. Although the opinions do not have the power of legislation or jurisdiction, they give a perception on how the European Directive is to be handled and thus have an impact on employees' privacy.

6.4.3 International Trade Unions

The International Labour Organization (ILO) was the first organisation addressing the issue of workers' privacy. In 1997, the first work on this topic by a union confederation was published: "Protection of Workers' Personal Data".[24] After that, it became rather silent around workers' privacy at the ILO. When the European Commission's consultation on the future legal framework of Data Protection Regulation was running in 2010, just a few European unions sent their statements – namely the Austrian and German union federations.[25]

The Union Network International (UNI Europa), a union federation in the service sector, concluded at an executive assembly in June 2010 that: "several reasons plead in favor of establishing a particular framework of employment specific rules: legal clarity and certainty, a more consistent and homogenous application of the rules governing the protection of individuals' fundamental rights and freedoms in this regard, the specificity of the employment relationship and the weaker position of workers, recent technological advances and their application in the workplace, the growing number of transnational mergers, take-overs and acquisitions and an increasing number of employees working for companies or organizations that have establishments or subsidiaries in more than one country, the growing tendency of multinational companies to concentrate personal data of all employees in one country and therefore undermine national participation rights of employees in the field of data storage, handling and processing."[26] UNI Europa already had basic experience in workplace privacy as it has been dealing with the issue since 1998, when the campaign "online rights @ work" was launched, which concluded in a code of practice in 2000.[27] The code, for example, includes that employees and their representatives must have the right to use ICT for union purposes and that hidden surveillance at workplace shall be forbidden. (This point showed up again when the EMPL committee voted on the GDPR in 2013.)

[24] International Labour Organization, *Protection of Workers' Personal Data* (Geneva, 1997).

[25] Österreichischer Gewerkschaftsbund, *Stellungnahme zum Gesamtkonzept für den Datenschutz der Europäischen Union* (Wien, 2011).

[26] Uni global union, *Data protection and employment in the European Union* (Madrid, 2010): 2.

[27] Uni global union, *online rights at work* (Nyon, 2000).

The European Trade Union Confederation (ETUC) followed with a document adopted in October 2012,[28] proposing that proceeding of workers' data needs distinct legislative framework: "In order to respect different labour market models and industrial relations system in Europe, the issue of data protection for workers should be regulated in a specific directive stipulating minimum standards that considers both the need for protection of workers' personal data and the role of trade unions when they act as a part of the collective bargaining process". This ongoing demand for specific legislation is not fulfilled within the GDPR, but another point – important to unions as well – was: the DPO. The ETUC appealed for "making the appointment of an independent DPO mandatory and harmonizing the rules related to their tasks and competences. In addition it would be advantageous to provide at European level adequate training standards for such officers."[29] DPOs are part of the GDPR-proposal of the European Commission, while the DPOs' training standards were added by the European Parliament Committee on Civil Liberties, Justice and Home Affairs (LIBE).

6.4.4 The European Economic and Social Committee (ESSC)

The opinion of the European Economic and Social Committee (ESSC) is close to that of the ETUC concerning workplace regulation although not claiming for an individual legal framework on the topic.

The first draft by the European Commission (Art. 82) said: "Within the limits of this regulation, Member States may adopt by law specific rules regulating the processing of employees' personal data in the employment context".[30] The ESSC expresses: "The words: 'Within the limits of this Regulation ... ' should be replaced with: '... On the basis of this Regulation ... '".[31] It can be reviewed as an success of the ESSC that this claim together with the amendments of the EMPL committee proposing the same are now part of the parliament's draft of the GDPR (see also Sect. 6.5.7).

Concerning the DPO, the ESSC defines a set of rules: "The conditions related to the role of DPOs should be set out in more detail, particularly in relation to protection against dismissal, which should be clearly defined and extend beyond the

[28] European Trade Union Confederation, *ETUC position in the General Data Protection Regulation – improving the protection of workers' data* (Brussels, 2012).

[29] European Trade Union Confederation, *ETUC response to the Communication from the Commission 'A comprehensive approach on personal data protection in the European Union* (Brussels, 2011).

[30] 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* (Brussels, 2012).

[31] European Economic and Social Committee, *Opinion of the European Economic and Social Committee on the General Data Protection Regulation* (Brussels, 2012).

period during which the individual concerned holds the post; basic conditions and clear requirements for performing this activity; exemption of DPOs from liability where they have reported irregularities to their employer or to the national data protection authority; the right for employee representatives to be directly involved in the appointment of the DPO and to be regularly informed about problems that arise and how they are resolved. The issue of the resources allocated to the function must also be clarified."[32] This detailed list is a clear indication for the importance the ESSC sees in this position. Some of the demands – such as the dismissal protection for the DPOs – can also be found in the LIBE proposal; however, only until the end of the officer's period. Still, the question of legal accountability of the DPO remained unsolved and employee representatives' participation rights are not strengthened at all. This consolidated version of the ESSC – consisting of employers' and employees' representatives – is considerable since it makes a commitment that workers' representatives have to be asked when a DPO is established.

6.4.5 The European Council

The European Council is just mentioned for the sake of completeness – to add the third party of legislation of the European Union. But since the European Council prefers closed-door negotiations, not much is known about its opinion – except for one communication in May 2013.[33] The German newspaper "Spiegel Online" reported on 2nd of December 2013 that the trialogue-negotiations could fail at all due to the German "waiting game" at the European Council.[34]

Summing up the employees' interest organizations and engagement of trade union in employee data protection over the last two decades, it can be depicted that there has been quite a lot of bargaining at company and branch level. Collective agreements concerning privacy at workplaces are drawn up by the social partners in several EU member states, some even on the branch level (Denmark, Italy and the Netherlands), and some actually on the national collective bargaining level (Belgian, Denmark, Norway). But just one member state has a specific legislation act on data protection regarding employment relations passed by parliament (Finland).

At the same time, there is not much further action from national unions when it comes to an international level. Here, we can depict that the torch is passed on to international union organizations such as UNI Europa or the ETUC. The higher the bargaining level gets, the less legal agreements by the social partners can be found.

[32] European Economic and Social Committee, *Opinion of the European Economic and Social Committee on the General Data Protection Regulation* (Brussels, 2012).

[33] Council of the European Union, *Interinstitutional File 2012/0011* (Brussels, 2012).

[34] http://www.spiegel.de/netzwelt/netzpolitik/deutsche-beamte-bremsen-europas-datenschutz-aus-a-936704.html

6.5 How the GDPR Affects Workplace Privacy

The European Commission drafted a new Data Protection Regulation, officially presented – after a leaked version in November 2011 – on 25th of January 2012. The following text only refers to those GDPR articles particularly relevant to the employment context. The European Parliament's Committee on Civil Liberties, Justice and Home Affairs (LIBE), responsible for the concluding amendments on the GPDP in October 2013 voted on it's GPDP-version after having dealt with almost 4000 amendments submitted by the members of parliament. In the following chapters I will point out which of the European Councils and which of the LIBE-committee's amendments underline the trade unions' position and strengthen workplace-privacy, and which contrast union's standpoints.

6.5.1 Harmonization

Interdependent corporate structures all over Europe and beyond require equal data protection standards. The European Data Protection Directive from 1995 tried to fulfill this task, but was not very successful as has been argued in Sect. 6.3. Data protection authorities, jurisdiction and sanction practice offered a wide range of data protection practice.

Currently, it is difficult to get access to employees' personal data in another country than that of data origin; not only being a matter of language. The possibilities of controlling data processing subsequent the data left its "home country" are more or less inexistent as we learn by consultation processes. These troubles of cross border data access are present not only for employees, but also for the management of multinational groups. Facing the complaints multinationals express concerning difficulties in transferring transnational data, one can easily conclude that there are not the same legal standards on data protection within the EU at that time. Thus, harmonization would support the needs of all parties concerned.

On the other hand, regarding differing labour law regimes and participation rights of workers' representatives across Europe, harmonization is fairly unrealistic. Common minimum standards (for example, how DPOs or official data protection authorities shall fulfill their duties) would give employees a more stable basis. Hence, it is an advantage to have data proceedings in the employment context equipped with further national possibilities (also see Sect. 6.5.7).

6.5.2 The Threshold

Since most of the European data protection laws do not know specific labour regulations, i.e. no specific regulation on DPOs at work or other specifications in the employment context, there was no need of thresholds excluding one or the other company. For some new responsibilities are transferred to undertakings, the European Commission set a threshold to some of them. The European Commission's version of GDPR fixed a threshold of 250 employees a company would need in order to be concerned. The "High Level Group of Independent Stakeholders on Administrative Burdens" established in 2007 by the European Commission might have been one of the drivers of the Commissions' GDPR proposal. Although, in Austria this threshold would lay the "burden" of a DPO at the company level on only 2 % of the companies, nevertheless employers' interest organizations strongly opposed. This again shows the unwillingness of employers to seriously deal with the topic. Just 16 % of Austrian companies voluntarily installed a DPO at the company level and this officer is not responsible for employees' personal data.[35]

The threshold designed by the European Commission comes into force, if data controllers not established in the European Union have to entitle a representative in Europe (Art. 25), if they designate a DPO at the company level (Art. 35), if they document data proceedings (Art. 28) and if it comes to sanctions (Art. 79).

The LIBE committee proposed another threshold in article 25: "a controller processing personal data which relates to less than 5000 data subjects during any consecutive 12-months period and not processing special categories of data [. . .] or data on children or employees in large-scale filing systems."[36] According to the LIBE committee's plans, a risk analysis should be implemented for companies below the threshold as well, but documentation duties should apply to all companies. The LIBE definition posts a more technical approach. It lays the emphasis not on company size, but on the companies' products, no difference whether these products are materials or services. The LIBE approach has a look on what the company does and not how big it is. Seen from an employee's interest perspective this facilitates law enforcement by the fact that employee data is declared valid, if it comes to obligatory establishing representatives of controllers, since this representative would be responsible for fulfilling the data subject's rights. Documentation duties for all companies and a newly defined threshold are a return to the employees' interest.

6.5.3 Consent

The LIBE proposal does no longer distinguish between consents given by a data subject under circumstances of equal power or under circumstances of unequal power, while the European Commission's draft did so. In recital 34, the Commission explicitly defined the employment relation as a relationship with imbalanced power,

[35] Clara Fritsch. "Vogelstraußpolitik, der Tenor von Umfragen zum innerbetrieblichen Datenschutz in Österreich." *Arbeit und Wirtschaft* (2008).

[36] Jan Albrecht, *Inofficial Consolidated Version after LIBE Committee Vote Provided by the Rapporteur* (Brussels 2013).

in which consent should not be a legitimate ground for data proceedings. This gave hope to employees and their representatives and interest organizations that the bad practice of blank consents would diminish. This optimism reduced after the LIBE voting.

6.5.4 Documentation

Until now, it was up to national legislation how to handle the transparency principle. Austria decided to implement a register open to the public, in which each data proceeding is to be recorded by the data controller – the employer in employment relations. The register, handled by the Austrian Data Protection Authority, helped works councils as well as employees to enforce their right on information, to force the employer to comply with the law. When it comes to data transfer to third countries or proceedings including sensible data, the Austrian authority actually had to approve proceedings, hence becoming an ally of employees and works councils, who do not want employees' data to leave the company in order not to lose access and controlling rights.

Documentation duties now are shifted to the company level by the GDPR (Art. 28). Although, the national authorities have the right to control these documentations (Art. 29), the anticipated practice – at least in Austria – is of only little usage concerning this right. Particularly, since it is evident that the Austrian authority holds the 23rd position out of 24 European member states when it comes to personnel resources.[37] The closure of the official documentation register in Austria will certainly weaken the employees' position.

6.5.5 Responsibility on the Company Level

A new pile of employer's responsibilities and legal data proceeding possibilities will find their way into employment relations: Data protection by design and by default (Art. 23), documentation at the company level (Art. 28), data protection impact assessment (Art. 33), data protection compliance review (Art. 33a), codes of conduct developed or at least proofed by the data protection authority (Art. 38), data protection certification (Art. 39) and binding corporate rules approved by the national data protection authority (Art. 43) shall now be available for employers to proof their data processing to be legal. Experience – at least in Austria – shows that self-made, self-controlled inner-company rules are likely to be weak, not to be followed and not to be sanctioned. Especially, if there is little participation and

[37] Hans Zeger, "Datenschutz International, Unterschiede, Gleichwertigkeit, Vereinbarkeit" (Vienna, 2007).

controlling power of employees' representatives and unions or at least of public bodies, one cannot really trust the self-regulation of companies. It seems as if the GDPR follows the already existing practice in some European countries where employer organizations wrote codes of conduct regulating employees' internet behavior on workplaces, e.g. in Ireland, Italy or Norway.[38]

The LIBE vote added just one of the new accountability tools to the co-determination rights of employees' representatives: When proceeding data by means of binding corporate rules, employers have to design these rules together with the employees' representatives or at least inform them about their existence (Art. 43/1a).

6.5.6 The Data Protection Officer

A compulsory DPO at the worksite, who performs his/her tasks independently and represents a gateway for employees, their representatives, employers and the data protection authority, was one of the most important demands expressed by the Austrian Trade Union Federation. Experts from Germany postulate this as well. Peter Schaar, the former German Federal Commissioner for Data Protection and Freedom of Information, states that the DPO is an essential addition to the European Data protection law. But Schaar adds that the DPO needs more protection from arbitrary actions by employers and needs to cooperate closely with employees' representatives.[39] The demand for a compulsory DPO at the worksite with dismissal protection is in coherence with the Europeans Commission's and the LIBE Committee's draft of the GDPR. The European Commission's proposal created the DPO not bound to employer's instructions, but without employees' representatives' participation or even information (Art. 35 ff). Only 2 % of Austrian companies would have had to install this position, since the Commission set a 250-employee-threshold (see Sect. 6.5.2).

Some amendments during parliamentary discussions of the Committee on Employment and Social Affairs (EMPL) also found their way into the LIBE proposal, such as the ban of secret surveillance or blacklisting. Other amendments of the EMPL were brought in on part of parliamentarians standing close to unions, advocating for more employees' representatives' participation rights, but did not survive the EMPL vote in February 2013.

LIBE amended a 4-year working period (Art. 35/7) instead of the 2 years proposed by the Commission, dismissal protection (Rec. 75), "the ability to work with employee representation [. . .], advanced training measures to maintain the specialized knowledge required to perform his or her duties" (Rec. 75a) as well as

[38] Catherine Delbar et al., "New technology and respect for privacy at the workplace," European Industrial Relations Observatory (2003).

[39] Peter Schaar, "Die geplante EU-Datenschutz-Grundverordnung, Auch beim Beschäftigtendatenschutz ist ein Nachbessern erforderlich", Computer und Arbeit (2013/3).

the task to inform employee representatives on data processing of the employees (Art. 35/1j). Hence, at least the recitals explain that DPOs also have to deal with employees' personnel data and serve as contact person for their concerns. This could strengthen employees' enforcement of the fundamental right to privacy.

6.5.7 The Article on Employment Relation (Art. 82)

From a union's perspective, the article on special data proceeding within an employment relation is one of the crucial parts of the GDPR. It was reworked by the EMPL and sets standards in employee data protection all around Europe for the first time. Although the GDPR now sets one standard for all European member states, it will be hard to match it with labour law regimes (compare Sect. 6.5.1). Having European minimum standards on dealing with employee data is a proper means to also take into account special national labour rights. It would have been of no use, if according to the GDPR – like the European Commission stated in its first draft – member states would have had to apply all the same level of workplace related data protection regardless of their national labour legislation. Especially participation rights of workplace representatives concerning collective agreements – whether on company, branch or regional level – would have been impaired by the GDPR.

What strengthens employee data protection within this article is the ban of blacklisting employees, who e.g. took part in union actions making it impossible for them to find work again and the ban of any hidden surveillance measures. Employers need to offer clear information and are allowed to precede personal data only if: "The purpose of processing such data must be linked to the reason it was collected for and stay within the context of employment. Profiling or use for secondary purposes shall not be allowed" (Art. 82/1a). What we still miss are workers' representatives' participation rights.

6.5.8 The One-Stop-Shop

Although a harmonized law concerning data protection at the workplace is a welcomed step further, the now installed principle of one-stop-shop will be a practical obstacle to protect employees' privacy rights. The "one-stop-shop", meaning that establishing one main company within the European Union providing one DPO for all other establishments, facilitates data transfer for companies. In principle, this could also make it easier for employees to enforce their data protection rights. They would not have to pass several authorities, would have a well-defined authority or other responsible person to address and could rely on being treated as all other European employees.

As consultant practice shows these advantages might be overridden by disadvantages such as: data subjects must first find out, who is responsible for their data protection requests – the bigger the multinational, the more complicated this is; especially within "matrix-organisations", a currently favoured organisation structure throughout multinationals. In matrix-structured companies the superior is no longer responsible for disciplinarian and professional tasks. The authorities are separated from each other and from their local connections. An employee may have his/her disciplinary superior two floors above and the professional superior some 2.000 km away at the mother company. Such company structures cause rising exchange of personnel data within the personnel management via ICT systems. Since labour law and therein inscribed participation rights of workplace representatives on the company level differ all over Europe – and beyond – it seems likely that multinationals will locate their main establishment in a country, where participation rights are rather week. Such regime shopping – quite common in matters of tax regulations – might then also occur in terms of data protection. This is already happening, for example, in Ireland, where there are low taxes and low data protection interests united and where big players in the worldwide web already have headquarters as the Financial Times reported on September 25th, 2013 (eBay, Facebook, Google, LinkedIn, Twitter, Yahoo, Accenture, . . .). While Ireland's data protection commissioner welcomes the one-stop-shop (according to the Financial Times on July 15, 2013), the experience users make when claiming for their right on information is that Irish data protection authorities are not supportive.[40]

6.5.9 Sanctions

The newly adopted sanction regime differs from the current one. Sanctions are no longer imposed according to a fixed amount but also according to a percentage share of the annual worldwide turnover (Art. 78 and 79) – similar to European competition legislation. The European Commission's draft included a maximum of 2 % of the worldwide turnover, while the LIBE voted for a maximum penalty of even 5 %. This, of course, alarmed enterprises and is definitely one explanation for the extraordinary high number of amendments to the GDPR.

When visiting Austrian companies for consulting reasons, one observes that multinationals start being concerned about high sanctions they might face according to the GDPR. Until now, it was regarded to be a trivial offense not to fulfill the requirements of the data protection law in Austria – in particular because there were no legal consequences. But due to the new European data protection regime and its future sanction fees, "these times will pass away" as a works council put it during recent consultation talks.

[40] For example the experiences of the NGO "Europe versus Facebook" (http://www.europe-v-facebook.org/DE/de.html).

6.6 Summary

General recognition of employees' data protection as a special form of data protection is a step forward. It is more than many EU member states currently offer their employees. An equal law across Europe – a DPO in many companies, specific regulations for the employment relation and higher sanctions – will add more value to employees' privacy.

Mutual efforts of employees' interest organizations (such as ETUC, UNI or the ÖGB) and the European social partners in the ESSC made some advantages possible for employees' data protection (such as the DPO, the ban of blacklisting, or the higher sanctions).

The current directives' proposal fulfils the employers' will of easier data transfers but it lacks the employees' right to easily access his or her personal data. Hence there is still an imbalance between employers' possibilities and employees' rights. The GDPR clearly fails regarding participation rights of workplace representatives for example, when it comes to establishing a DPO at the company level. Obviously, employee representatives' participation rights are shifted to the national level, but some minimum standards may improve employees privacy.

Bibliography

Albrecht, Jan, "Inofficial Consolidated Version after LIBE Committee Vote Provided by the Rapporteur" (published 22nd of October 2013, accessed February 12, 2014, http://www.janalbrecht.eu/fileadmin/material/Dokumente/DPR-Regulation-inofficial-consolidated-LIBE.pdf)

Article 29 – Data Protection Working Party, "Opinion on the Processing of Personal Data in the Employment Context, Executive Summary", published 2001, accessed February 1, 2014, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2001/wp48sum_en.pdf

Article 29 – Data Protection Working Party, "Working document on the Surveillance of Electronic Communications in the Workplace", published 2002, accessed February 1, 2014, http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2002/wp55_en.pdf

Busch, Klaus, Hermann, Christoph, Hinrichs, Karl und Thorsten Schulten, "Eurokrise, Austeritätspolitik und das Europäische Sozialmodell, Wie die Krisenpolitik in Südeuropa die soziale Dimension der EU bedroht.", Friedrich-Ebert-Stiftung, November 2012, accessed May 4 2014, http://library.fes.de/pdf-files/id/ipa/09444.pdf

Committee on Employment and Social Affairs, "Opinion for the Committee on Civil Liberties, Justice and Home Affairs on the proposal for General Data Protection Regulation", published March 4, 2013, accessed February 2, 2014 http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-%2F%2FEP%2F%2FTEXT%2BREPORT%2BA7-2013-0402%2B0%2BDOC%2BXML%2BV0%2F%2FEN&language=EN#title3

Council of the European Union, "Interinstitutional File 2012/0011", published 2012, accessed February 3, 2014, http://register.consilium.europa.eu/doc/srv?l=EN&t=PDF&gc=true&sc=false&f=ST%2010227%202013%20INIT

Delbar, Catherine, Mormont, Marinette and Marie Schots, "New technology and respect for privacy at the workplace." *European Industrial Relations Observatory* (2003), accessed February 4, 2014, http://www.eurofound.europa.eu/eiro/2003/07/study/tn0307101s.htm

European Commission, “Second stage consultation of social partners on the protection of workers’ personal data”, Brussels, 2002, accessed February 11, 2014, http://ec.europa.eu/social/main.jsp?catId=708

European Commission Directorate General Internal Market Unit E Media and data protection, “Special Eurobarometer, Data Protection”, Brussels, 2003, accessed February 4, 2014, http://ec.europa.eu/public_opinion/archives/ebs/ebs_196_en.pdf

European Commission, “The European e-Business Report, A portrait of e-business in 10 sectors of the EU economy, 5th Synthesis Report of the e-Business W@tch”, Brussels 2006, accessed February 4, 2014, http://ec.europa.eu/enterprise/archives/e-business-watch/key_reports/documents/EBR06.pdf

European Commission Direction General Justice Freedom and Security, “Flash Eurobarometer, Data Protection in the European Union, Citizens’ perceptions, Analytical Report”, Brussels 2008, accessed February 4, 2014, http://ec.europa.eu/public_opinion/flash/fl_225_en.pdf

European Commission Direction General Justice Directorate C Fundamental rights and Union citizenship Unit C.3 Data protection, “Summary of Replies to the Public Consultation about the Future Legal Framework for Protecting Personal Data”, Brussels, November 4, 2010, accessed February 4, 2014, http://ec.europa.eu/justice/news/consulting_public/0003/summary_replies_en.pdf

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)”, Brussels 2012, accessed February 4, 2014, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0011:FIN:EN:PDF

European Economic and Social Committee, “Opinion of the European Economic and Social Committee on the ‘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)’”, *Official Journal of the European Union C 229/90*, Brussels 31.7.2012, accessed February 1, 2014, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2012:229:0090:0097:EN:PDF

European Trade Union Confederation, “ETUC response to the Communication from the Commission ‘A comprehensive approach on personal data protection in the European Union’”, Brussels, 2011, accessed February 4, 2014, http://www.oegb-eu.at/servlet/BlobServer?blobcol=urldokument&blobheadername1=content-type&blobheadername2=content-disposition&blobheadervalue1=application%2Fpdf&blobheadervalue2=inline%3B+filename%3D%22EGB-Position_zur_Datenschutz-Richtlinie_%2528in_englischer_Sprache%2529.pdf%22&blobkey=id&root=S05&blobnocache=false&blobtable=Dokument&blobwhere=1294824487171

European Trade Union Confederation, “ETUC position on the General Data Protection Regulation – improving the protection of workers’ data”, Brussels, 2012, accessed February 4, 2014, http://www.oegb-eu.at/servlet/BlobServer?blobcol=urldokument&blobheadername1=content-type&blobheadername2=content-disposition&blobheadervalue1=application%2Fpdf&blobheadervalue2=inline%3B+filename%3D%22ETUC_Datenschutz.pdf%22&blobkey=id&root=S05&blobnocache=false&blobtable=Dokument&blobwhere=1353945635532

Fritsch, Clara. “Vogelstraußpolitik, der Tenor von Umfragen zum innerbetrieblichen Datenschutz in Österreich”, *Arbeit und Wirtschaft 04/2008*, Wien, 2008, accessed February 4, 2014, http://www.arbeit-wirtschaft.at/servlet/ContentServer?pagename=X03/Page/Index&n=X03_1.a_2008_04.a&cid=1208204202221

Haraway Donna, “Situated Knowledges: The Science Question in Feminism and the Privilege of Partial Perspective”, Feminist Studies, Vol. 14 No. 3, 1988

Harding Sandra, “Standpoint methodologies and epistemologies: a logic of scientific inquiry for people”, in UNESCO and International Social Science Council, 2010, pages 173–175. World Social Science Report: Knowledge Divides. Paris: UNESCO, accessed May 4 2014, http://knowledge4empowerment.files.wordpress.com/2011/06/harding_standpoint_-2010.pdf

Hendrickx, Frank. *Protection of workers' personal data in the European Union, Two Studies.* University of Leuven/Tilburg, 2002, accessed February 4, 2014, http://collection.europarchive.org/dnb/20070702132253/. http://ec.europa.eu/employment_social/labour_law/docs/dataprotection_hendrickx_combinedstudies_en.pdf

Hirsh, Elizabeth and Garry A. Olson, "Starting from Marginalized Lives: A Conversation with Sandra Harding", JAC, journal of Rhetoric, Culture, & Politics, 1995, accessed May 4 2014, http://www.jaconlinejournal.com/archives/vol15.2/hirsch-starting.pdf

International Labour Organization, "Protection of Workers' Personal Data", Geneva 1997, accessed 2nd of February 2014 http://www.ilo.org/wcmsp5/groups/public/---ed_protect/---protrav/---safework/documents/normativeinstrument/wcms_107797.pdf

Knorr-Cetina, Karin, *Manufacture of Knowledge* (Oxford 1981)

Mitrou, Lilian and Maria Karyda, "Employees' privacy vs. employers' security, Can they be balanced?", Elsevire Ltd. 2005, accessed February 4, 2014, http://www.icsd.aegean.gr/website_files/metaptyxiako/82038633.pdf

O'Rourke, Anne, Teicher Julian and Amanda Pyman, "Internet and Email Monitoring in the Workplace: Time for an Alternate Approach", *Journal of Industrial Relations* (2011 vol. 53)

Österreichischer Gewerkschaftsbund, "Stellungnahme zum Gesamtkonzept für den Datenschutz der Europäischen Union", Vienna, 2011, accessed February 4, 2014, http://www.oegb-eu.at/servlet/BlobServer?blobcol=urldokument&blobheadername1=content-type&blobheadername2=content-disposition&blobheadervalue1=application%2Fpdf&blobheadervalue2=inline%3B+filename%3D%22%25D6GB-Stellungnahme_zur_Datenschutz-Richtlinie.pdf%22&blobkey=id&root=S05&blobnocache=false&blobtable=Dokument&blobwhere=1294824487158

Riesenecker-Caba, Thomas and Alfons Bauernfeind. *Verwendung personenbezogener Daten und Grenzen betrieblicher Mitbestimmung: Datenschutz in der Arbeitswelt.* Arbeiterkammer Wien, 2011.

Schaar, Peter, "Die geplante EU-Datenschutz-Grundverordnung, Auch beim Beschäftigtendatenschutz ist ein Nachbessern erforderlich", *Computer und Arbeit* (Bund Verlag 2013/3)

Uni global union, "online rights at work", Nyon 2000, accessed February 3, 2014, http://www.uniglobalunion.org/sites/default/files/attachments/pdf/OnlineRightsAtWork_EN-print.pdf

Uni global union, "Executive Committee, Item 9, Data protection and employment in the European Union" (paper presented at the executive meeting in Madrid, June 2–3, 2010).

Uni global union "Submission to the European Commission communication A comprehensive approach on personal data protection in the European Union", Brussels, 2011, accessed February 7, 2014, http://ec.europa.eu/justice/news/consulting_public/0006/contributions/not_registered/uni_en.pdf

Zeger, Hans, "Datenschutz International, Unterschiede, Gleichwertigkeit, Vereinbarkeit" (paper presented at a seminar, Austria, Vienna, October 16–18, 2007).

Part III
To Forget or Not to Forget?
Or Is the Question: How to Forget?

Chapter 7
Timing the Right to Be Forgotten: A Study into “Time” as a Factor in Deciding About Retention or Erasure of Data

Paulan Korenhof, Jef Ausloos, Ivan Szekely, Meg Ambrose, Giovanni Sartor, and Ronald Leenes

Abstract The so-called “Right to Be Forgotten or Erasure” (RTBF), article 17 of the proposed General Data Protection Regulation, provides individuals with a means to oppose the often persistent digital memory of the Web. Because digital information technologies affect the accessibility of information over time *and* time plays a fundamental role in biological forgetting, ‘time’ is a factor that *should* play a pivotal role in the RTBF. This chapter explores the roles that ‘time’ plays and could play in decisions regarding the retention or erasure of data. Two roles are identified: (1) ‘time’ as the marker of a discrete moment where the grounds for retention no longer hold and ‘forgetting’ of the data should follow and (2) ‘time’ as a factor

P. Korenhof (✉)
Tilburg Institute for Law, Technology, and Society (TILT), Tilburg University,
Tilburg, The Netherlands
e-mail: P.E.I.Korenhof@uvt.nl

J. Ausloos
Faculty of Law (ICRI/CIR-iMinds), University of Leuven (KU Leuven), Leuven, Belgium
e-mail: Jef.ausloos@law.kuleuven.be

I. Szekely
Open Society Archives, Central European University, Budapest, Hungary
e-mail: Szekelyi@ceu.hu

M. Ambrose
Communication, Culture & Technology Department, Georgetown University,
Washington, DC, USA
e-mail: megLeta@gmail.com

G. Sartor
Law Department, European University Institute, Florence, Italy

Cirsfid, Law Department, University of Bologna, Bologna, Italy
e-mail: sartor@cirfid.unibo.it

R. Leenes
Regulation by Technology, Tilburg Institute for Law, Technology, and Society (TILT),
Tilburg, The Netherlands
e-mail: R.E.Leenes@tilburguniversity.edu

S. Gutwirth et al. (eds.), *Reforming European Data Protection Law*,
Law, Governance and Technology Series 20, DOI 10.1007/978-94-017-9385-8_7

in the balance of interests, as adding or removing weight to the request to ‘forget’ personal information or its opposing interest. The chapter elaborates on these two roles from different perspectives and highlights the importance and underdeveloped understanding of the second role.

Keywords The right to be forgotten • Data protection • Privacy • Internet • Time

7.1 Introduction

Tremendous advancements in information technologies have made it possible to capture, store and process vast amounts of data at marginal costs and in ways previously unimaginable.[1] Much of these data relates to specific individuals and may result in severe consequences. Moreover, the pervasiveness of modern networked communication technologies has given a global scope to these potential effects. Space and time are two key factors in the realm of increased accessibility and use of data, with significant, but different roles in the new digital world versus the old analogue world. Space and time are related; data accessible from anywhere but for no amount of time would reach no audience. The same goes for data that are accessible forever, but from nowhere. The “digital turn” implies an increased reach of information in both space and time, while information generally has a different value depending on the time and place.[2] This ‘disconnect’ increasingly causes issues. In this article we explore the extended reach of information in one of these two dimensions: time.[3] Time as a relevant factor in extending the reach of information was expressed by Rosen in his article with the telling title “The Web Means the End Of Forgetting”[4] and Mayer-Schönberger in his “Delete: the virtue of forgetting in the digital age”.[5] At the core of concerns in this domain is the potentially growing need of individuals to have certain information taken down or otherwise obscured. Or to use the controversial term that has taken central stage in the debate, to be “forgotten” – a term often used to express individuals’ desires to be free of information that already exists in the public domain, but that “with the passing of time becomes decontextualized, distorted, outdated, no longer truthful (but not necessarily false)”.[6]

The European Union is engaged in addressing concerns by developing regulation that enables individuals to oppose the persistent digital memory and giving them

[1] Cf. generally Mayer-Schönberger 2009.

[2] Cf. Ambrose 2012.

[3] As mentioned, time and space are related, but we will primarily focus on time.

[4] Rosen 2010.

[5] Mayer-Schönberger 2009.

[6] De Andrade 2012, p. 127.

a right to be forgotten (RTBF). Most notably this right – currently still under construction – is enshrined in the so-called "Right to Be Forgotten or Erasure", article 17 in the General Data Protection Regulation (GDPR) proposal.[7]

The introduction of the RTBF has been the topic of much – heated – debate. Rosen already dubbed the right "the biggest threat to free speech on the Internet in the coming decade".[8] However, next to numerous opponents, there are also many that underline the social necessity of a RTBF to limit access to persistent, personal, networked data.[9] The debate seems deadlocked with the adversaries taking almost absolute positions on the spectrum of forgetting versus remembering. Taking 'time' into consideration may allow for a more nuanced assessment. For instance, is it in the interest of freedom of expression and the marketplace of ideas to keep the opinion of a 14-year old recalcitrant adolescent in a school paper publicly accessible online for 10-years? What about 40-years? We can think of circumstances where we would answer such questions with 'yes', but equally important, we can think of circumstances where we would answer such questions with 'no'. Additionally, the answer that we as a society give to such questions may in return affect the interests at stake; if we decide that no utterance can ever be 'forgotten', debates may be stifled or curbed for fear of future consequences later on in life. Such considerations show that a pivotal role may be given to "time" in the balance of interests in cases where individuals aim to legally challenge persistent online memory. The main question of this chapter is thus:

What role can "time" play in the decisions and the balancing of different interests with regard to the retaining or removal of online available information?

This question was the focus of the "Timing the Right to Be Forgotten" panel at the 2014 Computers, Privacy and Data Protection conference in Brussels. The participants of this panel have collaborated to explore an answer to this question, which resulted in this chapter. It provides an analysis from the perspectives of the different panelists. After a brief introduction to the way we use digital information sources from an applied socio-philosophical perspective, we explore 'time' in law, followed by an analysis of discrete decision points in data processing and the data life cycle. Next we discuss how different interests can be balanced over time. The chapter concludes with a reflection on the insights obtained from the different angles. As the chapter discusses different perspectives provided by scholars from different disciplines, the style of the chapter is hybrid, which provides unique insight and broad treatment. All argue, in one way or another, that 'time' is an essential element to understand and manage information persistence in the digital world.

[7] The provision was introduced in the European Commission's *"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"*, COM(2012)11 final of 25 January 2012.

[8] Rosen 2012.

[9] Cf. De Andrade 2012, Mayer-Schonberger 2009.

7.2 The External Transactive Memory and Forgetting[10]

Before we explore time as a factor in the balancing of interests regarding data processing, we first need a model of (digital) memory and what 'forgetting' means in this context.

7.2.1 Memory, External Memory and Transactive Memory

Information is key to our functioning in the world – in relation to others and our environment. The ability to remember is a very important asset in this respect and the complex concept of 'memory' has been topic of research and debate in various academic fields.[11] The overarching similarity in these diverse fields lies in three process elements:

> Any memory system – whether physical, electronic, or human – requires three things, the capacity to encode, or enter information into the system, the capacity to store it, and – subsequently – the capacity to retrieve it.[12]

These three elements are intertwined: the way in which information is encoded determines what and how information is stored and this will in return determine what can be retrieved.[13]

Because the biological brain is perceptive to failures in its memory capabilities and has limited storage capacity, people make use of external tools to enhance their cognitive abilities and minimize their weaknesses.[14] Such tools can be used to alter, combine, transform and store information in ways that would be too time-consuming or complex to perform with the "naked" brain.[15] An all-familiar example of an external memory enhancement is an agenda, which complements the brain's limited memory capacity by diminishing the amount of information that it needs to process and store. Instead of remembering all our appointments, we only need to remember where our agenda is.

The praxis of external memory stores is heavily shaped by technology. The technology adopted determines what (written words, drawn pictures, photo's, voice samples) we can store, how much we can store (amount of books you can store in a house versus digital files on a personal computer) and how easily we can find it (searching manually versus search with a computer program in files). The "digital

[10] The line of thought described in this section has been explored previously in Korenhof 2014.

[11] Sutton 2012.

[12] Anderson et al. 2009, p. 5.

[13] Anderson et al. 2009, p. 5.

[14] Clark 2003, pp. 74–75.

[15] Clark 2003, p. 78.

turn" has dramatically affected the praxis. Practical limits of external memory stores have changed: we store increasing amounts of data,[16] can transport the information more easily[17] and are able to copy and distribute it flawlessly.[18] When publicly available on the Web, information is generally easily accessible to anyone with access to the right device and infrastructure, both of which are increasingly common. Search engines, apps and widgets effectively facilitate the retrieval of online information if its location is not already known.[19] With the "digital turn," our abilities to encode, store and retrieve information have thus expanded.

Treated as external memory, the Internet has an important characteristic not shared with other (private) external memories: because everyone can potentially add and retrieve information to and from the Internet, (particularly the Web) can function as a shared and socially interactive memory, a "transactive memory system".[20] Transactive memory concerns the structuring and processing of information within a group.[21] It is "a set of individual memory systems in combination with the communication that takes place among individuals".[22] In the transactive memory, the memory process elements of encoding, storage and retrieval are recognized to have "both internal and external manifestations".[23] The encoding of information within a transactive memory is done by individual agents or their external memory stores thus contributing to the shared memory. Individuals can retrieve information by consulting all available sources in the transactive memory, their own and other individuals' internal and external memory sources.[24] Using a transactive memory allows individuals to significantly enhance their (external) memory without the need for encoding and storing all information themselves.[25] A transactive memory shapes what a group of people remembers and influences what they individually take to be true.[26] The Internet is regularly used as a transactive memory and "has become a primary form of external or transactive memory, where information is stored collectively outside ourselves".[27] It thus shapes the manner in which we remember, and what we remember.

[16] Mayer-Schönberger 2009, p. 67.

[17] Van den Berg and Leenes 2010, p. 1112.

[18] Vafopoulos 2012, p. 411.

[19] Sparrow et al. 2011, p. 776.

[20] Sparrow et al. 2011.

[21] Wegner 1986, p. 185.

[22] Wegner 1986, p. 186.

[23] Wegner 1986, p. 188.

[24] Wegner 1986, p. 188.

[25] Wegner 1986, p. 188.

[26] Wegner 1986, p. 191.

[27] Sparrow et al. 2011, p. 776.

7.2.2 Forgetting and the External Transactive Memory

Humans have always used external memories, but with the adoption of information technologies, the mechanics of ‘remembering’ and ‘forgetting’ in the external memory process seem to have changed drastically.

Forgetting is a term generally used in relation to the biological brain and is a “fail[ure] to remember”,[28] a glitch somewhere in the memory process that either temporarily or permanently fails to retrieve specific information. It can be the result of failures in any of the three memory process elements, partial failures, temporarily failures or of failures in the elements combined.[29]

Forgetting in the human brain arises under the combination of various factors. Simplified, three main factors play a role in the occurrence of forgetting with regard to a specific piece of information: the passing of *time*, the *meaning* of the information and the regularity with which the information is *used*.[30] Meaningful and repeated use of information reinforces the persistence of the information in memory.[31] The passing of time weakens the strength of the memory of a specific piece of information.[32] Meaning, time and use thus jointly influence the persistence of information in memory, but each can also strengthen or weaken the others’ influence. For instance, information often loses value for us over time,[33] which increases the chance that it will be forgotten eventually because it will not be used.

Despite the fact that ‘forgetting’ is generally only used in relation to *human* agents, we think it is worthwhile to try and apply the term to the praxis of external memory stores. When regarding the concept of “forgetting” as a glitch purely on the *process level*, the term can also be applied to the external memory process, in which individuals *encode* and *store* information in the external memory store, and *retrieve* the information when they need it. Extending the term “forgetting” to the process as such can help us clarify and highlight the changes in the memory process mechanics that are caused by the praxis of external memory stores and provide guidance on how to implement “forgetting” in digital external memory.

Before the “digital turn”, “forgetting” usually occurred as the result of a necessary “forgetting-by-selection” decision because of storage space restrictions over time (i.e. one can fit only so many books in a library). People had to select what to keep —to externally “remember”— and what to eliminate from the storage space.[34] The praxis of memory thus transformed from a human memory store that

[28] Concise Oxford English Dictionary, 11th Edition.

[29] Dudai 2004, pp. 100–101.

[30] Dudai 2004, pp. 100/101.

[31] Dudai 2004, pp. 100–101.

[32] Dudai 2004, pp. 100–101.

[33] Ambrose 2012, p. 390.

[34] Szekely 2012, p. 349.

forgot-by-default, to external memory stores that generally remembered-by-default and required active forgetting-by-selection to make room for the most relevant information. With the "digital turn", this necessity to forget-by-selection drastically transformed and diminished, due to the continuous decline in storage space costs for digitally encoded information. In fact, the necessity for forgetting-by-selection has become so void, that often it is cheaper to get new or more storage space than to spend the effort to erase information. As some authors have already explored,[35] this led to a shift in the long-standing paradigm of human history: today remembering is natural, while forgetting has become an expensive and technically complicated business. This is most true for long-term declarative memory, both individual and collective, and more specifically, of data or document-based memory. But above all, this paradigm shift has relevance in the domain of digital memory, or at least computer-assisted memory.

As discussed in the introduction, there is growing opposition to "remembering-by-default" in certain circumstances and a call for some form of "forgetting" in external memories. The problem with fulfilling an individual's needs to "be forgotten" by an external networked memory store, is that it is not *the individual's* external memory store, but a transactive one. It is not the memory of a single agent that is at stake, but the external memory of multiple agents, each with potentially different interests in erasure or retention. The question is then how to balance the interests of these different agents in the decision to "forget" information in the external transactive digital memory. The way "meaning", "use" and "time" affect forgetting in the human brain may provide some guidance here.

"Time" is a factor that correlates with "forgetting" in the biological brain, and therefore a potentially relevant one if we are interested in facilitating "forgetting" in the digital transactive memory. Time is a fundamental dimension of the life of individuals, families, social groups and society as a whole, down to the survival of human culture. It is a fundamental dimension of memory and forgetting, too. Resources are freed up over time (potentially to be re-used[36]) and social needs to forgive and forget also take time into consideration. 'Meaning' and 'use' limit the memory decay which 'naturally' results from time lapse. The "digital turn" has undermined the technical need to forget, but not necessarily the personal and social need.

[35] For example, Mayer-Schönberger (2009) who was not the first but perhaps the most influential in realizing these changes, or Szekely (2012) who extended the framework of scholarly analysis to literary dimensions.

[36] Hadziselimovic et al. 2014.

7.2.3 Nuancing Persistence

Although the "[t]he Internet isn't written in pencil, it's written in ink",[37] and thus information permanence seems the rule, it is important to recognize the nuance of digital persistence. Information itself is not permanent, no matter the format. Digital information is particularly fragile. It requires a great deal of upkeep. Digital content is at the mercy of media and hardware errors, software failures, communication channel errors, network service failures, component obsolescence, operator errors, natural disasters, internal and external attacks, and economic and organizational failures.[38] This fragility has been the focus of digital preservationists who are deeply concerned about the "digital dark ages,"[39] "electronic crisis,"[40] and the "death of the digit."[41] Studies find various rates of decay, but they are dramatic ranging from rapid rates showing significant loss in days to about 10–15 % lasting a few years.[42] "If we are to understand the dynamics of the Web as a repository of knowledge and culture, we must monitor the way in which that knowledge and culture is managed. We find that the Web in its 'native form' is a far too transitory medium," stated Wallace Koehler while insisting that initiatives like Internet Archive are vital to cultural preservation.[43]

Having said this, it is apt to explore whether or not the 'natural' decay observed in these studies is sufficient to regulate in the name of permanence.[44] Content persistence in fact proves that the Internet is a lazy historian with no principled practices of preserving or protecting knowledge.[45] If online information is not more thoughtfully maintained as a collection, neither goals of privacy nor preservation will be met in the future. Tinkering about mechanisms to augment the external transitive memory fits this aim.

Psychologists distinguish between short, intermediate and long-term memory, internal and external memory, visual, auditory and conceptual memory, procedural and declarative memory. Relating to these and their different (temporal) characteristics, it is possible to distinguish short, intermediate and long-term forgetting,

[37] "The Social Network" (Columbia Pictures 2010, http://www.imdb.com/title/tt1285016/), quoted in Ambrose 2012 (Mark Zuckerberg is explained how permanent and harmful this aspect of the Internet is by his girlfriend, as she breaks up with him).

[38] Gladney 2007, p. 10.

[39] MacLean et al. 1998.

[40] Rosenzweig 2011.

[41] Feeney 1999.

[42] Ambrose 2013, citing: Gomes and Silva 2006.

[43] Koehler 2004.

[44] A particular problem with relying on natural decay is that data disappears from the Web at the whim of the data controller, not the data subject or the public. Valuable data is lost everyday while innocuous and harmful data remains. *See* Ambrose 2012.

[45] Ambrose 2012.

oblivion, or even amnesia alike. These types of memory and forgetting have their own characteristic time periods and even their names sometimes reflect the length of their sphere of interpretation. If this is true, why not speak about computer-assisted forgetting?[46]

If we want to – or question whether we should – limit the reach of the digital memory we may need to re-introduce 'time' into the equation (of time-meaning-use). A primary question here is whether time plays an independent role, or whether it affects a balance of interests. We will explore this question from different perspectives, starting with the law because of its importance in regulating behavior, also in the domain of data processing.

7.3 Time in Law

This section briefly sets out the weight and role time has in evaluating a person's right to have certain information taken down. Rather than giving a detailed analysis of the relevant legal provisions and case-law, it provides a *tour d'horizon* in a European context.

7.3.1 Removing Online Content

Individuals who want to have certain information taken down have reached for technological tools and pressed corporations to provide them with concrete deletion options. In many situations, however, these solutions do not result in satisfactory outcomes for the individuals involved and as a result, they are turning to the law to find relief. Although privacy and data protection law might seem the most straightforward legal frameworks in this context, many other legal domains could be relevant (i.e. defamation law, intellectual property law, general tort law, etc.). For the purposes of this section, we focus on the role of time in the context of privacy and data protection law in particular. Not only do these constitute the most relevant legal frameworks with regard to the issues dealt with in this chapter, but also do most of the other legal regimes have specific criteria in place for assessing the legitimacy of a takedown-request (e.g., wrongfulness, public dissemination, harmful intent, etc.) in which time plays a lesser role.

[46] In fact there exist computer-assisted forgetting tools and technologies, from specific Privacy Enhancing Technologies (PETs) to user-centric identity management systems, however, their capacity and spheres of use differ greatly and they are far from being commonly used.

7.3.2 Terminological Issues

The term “Right to be Forgotten” is used in the context of privacy and data protection law. It may not come as a surprise that the concept is subject to different interpretations, which – in turn – have led to a great deal of controversy.[47] Without going into details on this, it is worth highlighting one key distinction. The right can either be grounded on the general right to privacy – in which case it can be referred to as the right to oblivion (in French, *droit à l'oubli*) – or it can be based on the data protection framework – in which case it can be referred to as the right to erasure. Time plays a role in both situations.

7.3.3 Role of Time in the General Right to Privacy

In the movie Men in Black,[48] the protagonists use “neuralizers” to eradicate (short-term) memory of witnesses to alien incidents. It is not hard to see how the right to oblivion seems to be the translation of this technical tool into law. Its terminology suggests an obligation on third parties to remove certain information from their memory. Courts have recognized a ‘right to be forgotten’ based on the general right to privacy – inscribed in the ECHR (art. 8) and Charter of Fundamental Rights (art. 7) – in a number of cases.[49]

Looking at European case law in particular, the right has mostly been applied in order to shield individuals from being confronted with certain aspects of their past in a disproportionate, unfair or unreasonable way.[50] The textbook example undoubtedly is the ex-convict who sees his/her name popping up in the media years after the facts. This has become particularly relevant in the context of the digitization of newspaper archives. Quite recently, the European Court of Human Rights (ECtHR) has called attention to the concerns related to online availability of more and more information. In *Delfi AS v Estonia,*[51] the Court stated that “the spread of the Internet and the possibility ... that information once made public will remain public and circulate forever, calls for caution.”[52] In *Österreichischer Rundfunk v Austria,*[53] the ECtHR specified that the lapse of time since a conviction and release constitutes an important element in weighing an individual's privacy interests over

[47] Ambrose and Ausloos 2013.

[48] Columbia Pictures 1997, http://www.imdb.com/title/tt0119654/.

[49] Graux et al. 2012.

[50] Ambrose and Ausloos 2013.

[51] *Delfi AS v Estonia*, ECtHR, Application nr. 64569/09, 10 October 2013.

[52] *Delfi AS v Estonia*, ECtHR, Application nr. 64569/09, 10 October 2013, N92, pp. 108–109.

[53] *Österreichischer Rundfunk v Austria*, ECtHR, Application nr. 35841/02, 7 December 2006.

the public's interest in publication (n°68).[54] It may come as a surprise that the ECtHR has also applied the time-element as an argument *against* the RTBF. In *Editions Plon v. France,*[55] the heirs of former French President François Mitterrand had opposed to the publication of a book by the ex-President's private doctor. The ECtHR ruled, however, "the more time that elapsed, the more the public interest in discussion of the history of President Mitterrand's two terms of office prevailed over the requirements of protecting the President's rights with regard to medical confidentiality."

In short, the right to oblivion is primarily invoked in situations where an individual's personal life is publicly exposed. A careful balancing exercise with other fundamental rights will therefore be imperative. In striking this balance, time may play a determinative role, though not necessarily in favor of removing the information.

7.3.4 Role of Time in Data Protection Law

The application of the Right to Erasure – vested in the European data protection framework – seems much more straightforward, at least in theory. According to Article 12 of the Data Protection Directive 95/46 (DPD), data subjects have "the right to obtain from the controller [. . .] the erasure of data the processing of which does not comply with the provisions of this Directive".

For the purposes of this section, the right to erasure in Article 12 can be summarized as being applicable whenever the controller either fails to fulfill its obligations or ignores data subjects' rights. Keeping in mind the focus of this chapter, three elements in the data protection framework are relevant here: (a) the need for a legitimate ground, (b) the purpose limitation principle and (c) the data subject's right to object.

First of all, the processing activities will permanently have to be tested against the legitimacy grounds in article 7 of the Directive. Particularly the first and last justifications are interesting in this regard. When the processing activities are based on the data subject's consent, the controller will have to stop further processing upon withdrawal of consent. The Article 29 Working Party has specified, however, that such withdrawal can only be exercised for the future.[56] Only when the controller cannot present any other legitimate ground for *further* processing, can the subject

[54] Eventually, it was decided though, that the national court had given too much weight to the time-element. n°69 "The domestic courts attached great weight to the time-element, in particular to the long lapse of time since Mr S.'s conviction, but did not pay any particular attention to the fact that only a few weeks had elapsed since his release."

[55] *Editions Plon v. France*, ECtHR, Application nr. 58148/00, 18 May 2004.

[56] Article 29 Working Party, Opinion 15/2011 on the definition of consent 01197/11/EN WP187, at 33. http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp187_en.pdf.

request erasure of the data. The last legitimacy ground, however, constitutes an incredibly wide safety net controllers can fall back on. According to this ground (art. 7f DPD), personal data can be processed for as long as is "necessary for the purposes of the legitimate interests pursued by the controller (or by the third party or parties to whom the data are disclosed), except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject". It goes without saying that this "balance of interests" gives a lot of leeway to the controller and is hard to contest by data subjects. Nevertheless, this balance might oscillate over time, at least in theory.

Second, the purpose specification principle (article 6) constitutes some sort of benchmark against which the processing of personal data will be assessed over time. Besides having to be specific and explicit, the purpose also has to be legitimate. Whereas the specificity and explicit nature will normally only be relevant at the start, the legitimacy requirement will be more susceptible to the passing of time. In its Opinion on Purpose Limitation, the Article 29 Working Party specified that the processing must – at all different stages and at all times – be based on at least one of the legal grounds.[57] This requirement, the Opinion continues, goes beyond the scope of the legitimacy grounds in article 7 and implies the purposes for processing "must be in accordance with all provisions of applicable data protection law, as well as other applicable laws (e.g., employment law, contract law, consumer protection law, etc.)."[58] It concludes by saying that "the legitimacy of a given purpose can also change over time, depending on scientific and technological developments, and changes in society and cultural attitudes." On top of the potentially wavering nature of the legitimacy requirement, the personal data itself might also become unnecessary, irrelevant or inadequate to achieve the original (or a compatible) purpose.

Third, in principle the right to erasure can also be invoked when the data subject has successfully exercised his/her right to object. But, in order to do so, the subject will have to put forward compelling and legitimate grounds. In this regard, 'time' can both be such a ground, as well as a factor that changes the weight of the arguments for or against the right to object.

Although the data protection directive has been the subject of several cases before the Court of Justice of the European Union (CJEU) already, the right to erasure

[57] Article 29 Working Party, Opinion 03/2013 on purpose limitation, 00569/13/EN WP203, pages 19–20.

[58] The Working Party further elaborates that legitimacy also has to be tested against: "all forms of written and common law, primary and secondary legislation, municipal decrees, judicial precedents, constitutional principles, fundamental rights, other legal principles, as well as jurisprudence, as such 'law' would be interpreted and taken into account by competent courts.

Within the confines of law, other elements such as customs, codes of conduct, codes of ethics, contractual arrangements, and the general context and facts of the case, may also be considered when determining whether a particular purpose is legitimate. This will include the nature of the underlying relationship between the controller and the data subjects, whether it be commercial or otherwise."

has never really been dealt with directly until the so-called *Google Spain* case.[59] In this case, the CJEU was asked whether or not search engines fall within the DPD's (material and personal) scope of application and/or whether they are subject to the right to erasure with regard to the personal data they refer to. According to the original plaintiff in this case, some of the Google Search results when entering his name are not relevant anymore (i.e. links to an article on his bankruptcy proceedings).[60] The *Audiencia Nacional* (referring court) acknowledged that today, it is possible to create very detailed personal profiles in just a couple of clicks, with information that used to be difficult to find. The lack of territorial and temporal limitations to the dissemination of information constitutes a danger to the protection of personal data. The Spanish Court further specified that originally lawful and accurate personal data may become outdated overtime in the face of new events. Some of this information might actually generate social, professional or personal harm to the individual concerned. Indeed, one might claim that the impact of search engines (among others) is such that individuals are perpetually overshadowed by certain past events/facts that might not accurately – or in a proportionate way – represent their current capabilities. It could even be argued that with the right search terms, practical obscurity on the Internet is a myth.

Concerns over perpetual storage of (personal) data have also manifested themselves in the context of another legal framework before the CJEU. In *DRI & Seitlinger,*[61] the Data Retention Directive 2006/24 was at stake. The Directive

[59] CJEU C-131/12, still pending at the time of writing. This case involved a Spanish individual that had been subject to bankruptcy proceedings in the nineties. Spanish law required a local newspaper (LaVanguardia) to publish information on the public auction resulting from the bankruptcy. Upon digitizing its archive, links to this information popped up in Google Search results when entering the individual's name. The individual addressed himself to the Spanish data protection authority, requesting the removal of the article and search results. The DPA denied the request vis-à-vis the newspaper (as it had a legal obligation to publish the information in the first place) but did order Google to remove the link from its search results. The search giant appealed and the *Audiencia Nacional* referred some of the questions raised to the CJEU.

[60] Some say that the market may take care of the problems the RTBF seeks to address. Google's Eric Schmidt, for instance, writes that employing the services of an "identity manager" to maintain one's online presence will be "the new normal for the prominent and those who aspire to be prominent" (Schmidt 2013). Reputation services, as these identity managers are often called, can be paid by data subjects to move search results to pages beyond the effort of most searches. In order to move pages with content detrimental to the data subject to such an obscure rank, reputation services will flood the Web with content about the data subject. We find this solution to the problem unsatisfying for three reasons. The reputation service requires that a mass amount of data be presented about an individual, which is a problematic solution for anyone seeking to be 'left alone.' Additionally, these services are constantly battling search engines who do not appreciate their systems being gamed. Finally, this practice represents poor treatment of such a valuable information source. The only option for data subjects should not be to dilute the Internet with fluff.

[61] Judgment – 08/04/2014 – Digital Rights Ireland and Seitlinger and Others Case C-293/12 (Joined Cases C-293/12, C-594/12), http://curia.europa.eu/juris/document/document.jsf?text=&docid=150642&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=52531.

specified a data retention period between a minimum of 6 months and a maximum of 24 months. The Court decided that EU legislation exceeded the limits imposed by the principle of proportionality in Articles 7, 8 and 52(1) of the Charter, inter alia, because the retention period is relatively open while it must be based on objective criteria in order to ensure that it is limited to what is strictly necessary.

7.3.5 Two Roles 'Time' Can Fulfill in Law

It is hard to draw clear conclusions regarding the role of 'time' vis-à-vis the RTBF in a privacy and data protection context. What can be said, however, is that the concept seems to play two parts. Either, and commonly, time is a factor adding (or removing) weight to the request to removing personal information or its opposing interest (e.g., public interest), resulting in tipping the balance in either direction. Generally, the older information is, the less valuable retaining it is. The second role time can play is as the marker of the tipping point when the grounds for retention no longer hold and erasure of the data should follow. Passing an agreed retention period for data is a case in point. Sometimes, however, it is not so much time itself that causes the flip, but rather some other conditions being met at some point in time. This is the case where the purpose limitation principle is at play. Once the stated purpose is reached, there is no longer a legitimate ground for data retention, and hence from that moment in time onwards, data retention is no longer legitimate. This second role of time (time as boundary marker) especially comes to the fore in Article 17 of the proposed GDPR. In the Commission's proposal, data subjects will be able to invoke the right when the data are "no longer necessary in relation to the purposes for which they were collected/processed" or when the predefined storage period has expired.

Before we discuss the former role of time (as a weight in a balance of interests), we first explore time in its role as discrete tipping point in the discussion whether personal data should be retained or deleted.

7.4 Law, Time and the Use of Information: Specific Points in Data Processing

In this section we explore the life cycle of the creation and use of data and information and we highlight situations in which the decision of whether or not to create/retain/delete data is relatively straightforward. We identify specific points in data processing, which also denote specific points or periods in time, where enforcing of RTBF is reasonable or even necessary. Since data protection law and specific rules concerning data processing, are codified, it is easy to find legal arguments for interpreting these specific points. However, it should be emphasized that such legal arguments can only be interpreted in a constitutional, rule-of-law democracy, or in a narrow sense, in the legal system of the EU. Nevertheless, there are also moral arguments and fundamental values, which may be evoked to support these legal arguments.

7.4.1 (Moment in) Time as a Discrete Boundary for Erasure/Retention

7.4.1.1 Before Recording of Information Takes Place

Prior to the actual collection and further processing of personal data, a decision can be made not to collect the data in the first place. Data that are not collected do not require a decision to delete or retain data later on. The time preceding data collection decision therefore is relevant for our purposes. For example, if someone wants to make a photo or video recording of someone else’s activity, and the data subject realizes the preparations, the subject may ask him not to do so. The subject generally has a right and moral arguments to support his demand, although there are situations when this preliminary step cannot be applied: if someone actively participates in a street demonstration, he cannot demand recording of his participation not be made – he has become, even if temporarily, a public figure, performing public functions, and his activity is information of public interest, even if in a formal sense it can be regarded as his personal data. He cannot discriminate certain media either; he cannot distinguish friendly and adverse reporters or television channels.

7.4.1.2 Immediately Upon Recording

If the data subject discovers that his personal information is being, or has just been, recorded, he may demand the immediate deletion of the information, thus preventing the spread of the recorded information. The ubiquity of information recording devices nowadays implies that individuals can be part of such a scene instantly and constantly in particular (but not solely) in public spaces. Although there is pressure from the data industry to record and distribute ever more personal information, the moral right to object to such recordings is acknowledged. For instance, in some non-European countries where legal protection is weaker, the industry has accepted a de-facto norm that recording equipment make a shutter-click noise that cannot be turned off in order to call data subjects’ attention.[62]

[62] Smartphones manufactured and purchased in Japan or South Korea have this well-known feature, and lawmakers seem to have declared programs disabling the shutter sound illegal, see for example http://www.unwiredview.com/2012/04/20/south-korea-to-ban-cameraphone-shutter-sound-removers/ or http://news.asiaone.com/News/Latest+News/Science+and+Tech/Story/A1Story20111214-316106.html.

The mainstream (printed and electronic) media have traditional privileges in recording and distributing personal information. This is partly reflected in the press law, partly in the practice of courts in press-related lawsuits, and partly in the codes of ethics of the media. Typically, the media are allowed to record information on identifiable persons in public spaces, for example as part of a long shot, however, zooming in on individuals and recording this information is allowed only if consented by the persons concerned.[63]

Again, this demand for deletion of the recorded information cannot be applied when the data subjects perform public functions.

7.4.1.3 When a Legal Deadline Expires

Under the data protection regulation, data controllers can lawfully process personal data (provided the other requirements are met, see Sect. 7.3) as long as they are necessary for specified purposes. This may include being able to prove the existence of a relationship between parties after the primary relationship ended (e.g., contractual obligations completed). After this period there is no legitimate ground for retaining the data. In criminal law, information on prior convictions is kept in official registers until the expiry of the time prescribed by law, after which no detrimental legal effects shall apply on prior convicts. Similar expiry dates apply to minor offences, too. After these dates the data subject may receive a clean certificate of good-conduct. The expiry of such deadlines generally imposes an obligation on the data controller to delete the data. The concerned person may also require the deletion of her data forwarded earlier to other data controllers.

7.4.1.4 When the Conditions of Lawful Data Processing Are Not Met

In some cases processing of personal data takes place without meeting the conditions of lawful data processing as prescribed by data protection law. Such situations may occur, for example, when a data subject withdraws her consent and her data is retained and used nevertheless, or the purpose of processing does not exist anymore. In these cases, time is not an autonomous factor, but the legitimacy of data processing is limited in time (in hindsight). A complicating factor here is that data subjects may sometimes realize the non-compliant processing only ex post facto.

[63] As a main rule, the media can record such information under *prior* consent of the people concerned, however, there are some exceptions when asking for prior consent would spoil the situation. In such cases consent should be obtained right after the recording is made, on the spot – and if the consent is not given by the subjects, the recording should be deleted immediately. Well-known examples of such a situation are the candid camera type programs, when only those recordings can be seen on television, which the victimized subjects consented to after realizing the fact of recording (and that is why all such broadcasted episodes end with laughter, and not with angry reactions).

A special case occurs when a person objects to the processing of her personal data in the area of direct marketing. Many direct marketing laws obligate data controllers (the marketers) not to delete such data, but to put them on a separate list, the so-called Robinson list. The purpose of such a list is to filter out the "Robinsons" and not target them in subsequent marketing runs. As in the previous cases in this category, the legitimacy of processing here is in a sense limited in time. There, however, is no right to erasure after this point, but only a sort of "filtered use" of the subject's data in the future.

7.4.1.5 At Pre-defined (or Default) Dates

Comprehensive user-centric identity management systems like PRIME[64] envision a network of compatible data processors within which rules set by laws and individual contracts, or defined by data subjects themselves, are automatically enforced. For example, if the data subject posts a photo to a social network site for two weeks only, after this date the photo will automatically be deleted (and not only from the primary data processor but also downstream from all systems adhering to the same standard). Despite working prototypes, PRIME(-like) infrastructures on a large scale are still only a dream.

From a different perspective, Mayer-Schönberger suggests a related idea: each piece of personal data should have an expiry date after which it should automatically be deleted.[65,66] Such expiry dates may be defined as default characteristics of the data processing system, but may also be defined individually by the data subject. The expiry dates may be changed before the deletion of the data.

7.4.1.6 Grey Zone: Data of the Deceased

Death is the ultimate turning point in people's life, marking the end of being a legal subject, however, not necessarily meaning the end of remembering the deceased person. In most legal regimes the data relating to the deceased are not personal data in the strict sense of the word,[67] although the virtually indelible data of the deceased

[64] Privacy and Identity Management for Europe, http://www.prime-project.eu. See also Camenisch et al. 2011.

[65] Mayer-Schönberger 2009.

[66] A practical application of this notion can be found in the popular social media application Snapchat, where users can upload images ("Snaps") that are visible to recipients for a period from 1 to 10 seconds to be decided by the poster.

[67] For instance, art. 2a of the Data Protection Directive 95/46/EC limits personal data to natural persons, which ties the scope to legal personality in civil law. In civil law legal personality terminates at death. See also Art. 29 Working Party Opinion 4/2007 on the concept of personal data, 01248/07/EN, WP136, p. 22. The Working Party discusses some special cases where data of the deceased indirectly receive some protection.

may revolve in web-based services for a long time. In the case of the deceased, the RTBF can only be enforced by surviving relatives. In this case it is not the protection of personal data but the protection against the injury to the memory of a deceased person which may be applied, and the relatives are entitled to file for court action.

We can imagine the history of data relating to a deceased person as an ever fading grey zone, or a virtual trail of a comet, which at the beginning (at the luminous nucleus of the comet) is very close to the personality of the deceased, and through the passing of time becomes mere historical data, gradually losing its personal nature.[68]

It should be noted that data relating to the deceased may also relate to the surviving relatives and hence the decision whether or not to erase the data depends on more factors than just the interest of the deceased.

7.4.1.7 Never

There are cases when RTBF can never be enforced lawfully. This is the case of personal data of persons performing public tasks, generated in connection with their task. These data are strictly speaking personal because they relate to an identified or identifiable natural person, but the person is treated as an institution rather than as an individual and the public interest prevails over the private interest of the individual. Similarly, personal data lawfully published in the media cannot be erased either. It is questionable whether this rule applies to online media, too, since a fundamental purpose of the RTBF is exactly to counterbalance the unintended consequences of using new media.

7.4.1.8 Special Case: Memory-Preserving Institutions

This case represents one of the most controversial domains of RTBF: forgetting in archives and other memory-preserving institutions. The international archiving community has strongly opposed the enactment of art. 17 GDPR.[69] Administrative archives are operating under legal obligations, which are at odds with a right to be forgotten or erasure for data subjects. Historical type archives (in particular the ones collecting documents on recent history) are meant to preserve history for the benefit of the future. Removing personal data from the archives infringes upon this purpose. Hence it comes as no surprise that, according to the draft EU Regulation, RTBF shall not apply to the extent that processing of the personal data is necessary for historical, statistical and scientific purposes.

[68] In the age of Facebook profiles, avatars and Internet archives this fading of personal nature is less and less obvious, and the questions of post-mortem privacy has become a growing research area, see for example Harbinja 2013 and Edwards and Harbinja 2013.

[69] See the declaration of the Association of French Archivists 2013.

7.4.2 Use and Time

This section has elaborated on discrete moments in time in which it is relatively clear whether personal data can be retained or has to be deleted. The interests of the data subject who wants their data be removed are at the core in the cases elaborated. In most cases discussed, only the data subject (or relatives in case the data subject is deceased) and the data controller hold acknowledged interests. The examples have focused on the immediate information needs of these parties. The use of information by third parties seems to only be acknowledged in the special case of the memory preserving-institutions (in which the information already has a context-specific meaning). Remote information needs, be it from archivists who aim to preserve our times for future historians or from predictive analytics which may improve health care, or from entrepreneurs who want to have legal certainty regarding the reputation and creditworthiness of their business partners, also play a role in RTBF decisions. Third parties use the information in the external transactive memory and may rely on it. It is here where a balance of interests needs to take place leading to deleting or retaining certain personal data. Time, as said, plays a role in this balance as a contributing or limiting factor. In the following section we elaborate on the role of time with respect to 'use' and 'meaning'. We will look at the meaning of information in its data life cycle, and the changing balance of different interests in time.

7.5 Balance of Interest Over Time

It has been said that the RTBF "is based on the autonomy of an individual becoming a rightholder in respect of personal information on a time scale; the longer the origin of the information goes back, the more likely personal interests prevail over public interests."[70] In this section we take a closer look at the balance of interests over time, where the passing of time influences the meaning and use of information by different parties, and thereby affects the balance of their interests.

7.5.1 Changing Balance of Interests: Data Life Cycles

In order to shed some light on the manners in which the balance of interests can change over time, we shall group the interests involved in data protection cases into two sets. On the one hand the *pro-processing interests*, which include all legally relevant interests promoted through the processing of the personal

[70] Weber 2011.

data at issue, and on the other hand the *con-processing interests*, which include all legally relevant interests that may be demoted by the same processing. Pro-processing interests may comprise diverse meanings and usages of information, such as economic and non-economic goals, and right and values, such as economic freedom, efficiency, property interests, security, freedom of expression, freedom of information, transparency, democracy, and equal judicial protection. The most important pro-processing interests are based on the meaning data hold for the public, the values currently secured in the exceptions of Art. 17(3) of the proposed GDPR that allow for retention of data: (a) to protect the right of freedom of expression; (b) for reasons of public interest in the area of public health; (c) for historical, statistical and scientific research purposes; (d) for compliance with a legal obligation to retain the personal data by Union or Member State law.[71] Con-processing interests similarly may include not only privacy and data protection rights strictly understood, but also the rights to private life, identity, self-determination, non-discrimination, a fresh start, protection from unwanted intrusions, dignity, etc.

We model the changing balance of pro-processing and con-processing interests in a graphic form, as in Fig. 7.1. The horizontal axis represents the passage of time, from the initial moment when the processing has started (t_0). The vertical axis represents the *legal impact* that the processing has with regard to the *pro* and *con* interests. The full curve represents the importance of positive impact on pro-interests and a dotted curve represents the importance of the negative impact

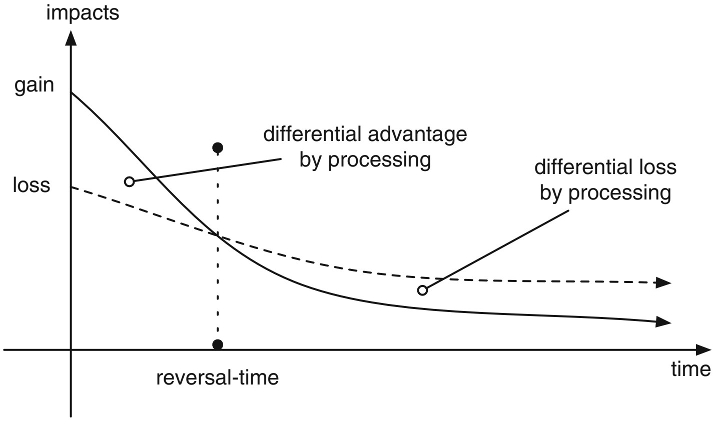

impacts
gain
loss
differential advantage by processing
differential loss by processing
reversal-time
time

Fig. 7.1 The impact of processing (*line*) and non-processing (*dotted line*) over time

[71] DRAFT EUROPEAN PARLIAMENT LEGISLATIVE RESOLUTION on the 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)0011 – C7-0025/2012 – 2012/0011(COD)) adopted in the first reading of the Parliament on 12 March 2014.

on con-interests. The curve over time is the expression of the data's life cycle; "information as it changes value through the full range of its life cycle from conception to disposition."[72]

For instance in Fig. 7.1, at t_0 the curve corresponding to pro-interests is much higher than the curve corresponding to con-interests. This means that at t_0 the positive legal impact which the processing provides by promoting certain interests is much higher than the negative legal impact that the same processing causes by diminishing the data subject's privacy. Therefore, processing at t_0 provides a net benefit all things considered. Consequently, a regulation permitting it also has a positive legal impact, all things considered.

We shall here focus on cases where the originally prevailing pro-processing interests are outweighed at a later stage by con-processing interests. This happens in particular when the personal information is distributed online for purposes pertaining to journalism, or more generally to freedom of expression. In such cases, there is generally a continuous diminution in the importance of the distribution of information with regard to both pro- and con- processing interests, up to the tipping point. This is because public interest, more aptly called public intrigue here, is quite fleeting, and thus the public meaning and use of information is equally fleeting. Entering any number of momentary Internet snafus (e.g., Alexandra Wallace, Caitlin Davis, Justine Sacco) reveals spikes in search activity over a matter of weeks and then a sharp drop back to insignificance.[73] The 'newsworthiness' of content generally protects the public's right to access the information.[74] Like data freshly created (e.g., current address, purchases, body measurements) this information is relatively current, contextualized, and new before it becomes outdated, uncontextualized, and condensed or aggregated. Older personal facts are generally less meaningful for both the public and the data subjects and are thus also less used. In particular, older information about a person usually gives a less relevant clue to what and who a person "is" now, and therefore should in general be less meaningful, both for those who want to know about that person and for the person herself. There are, obviously, deviations from these general trends where certain past information suddenly may become more important to the public and/or more damaging to the data subject.[75] For instance, when data subjects apply to elective political positions, their data concerning any past criminal or inappropriate behavior becomes more meaningful to the public. Here, we shall just consider the more common case when there is a continuous decrease in the importance of impacts on both pro- and con-processing interests. Consider for instance those cases where personal information related to

[72] Hill 2009, p. 57.

[73] See Ambrose 2012, p. 413 for examples taken from http://google.com/Trends.

[74] "Newsworthiness" varies across jurisdictions. *See* e.g., *Time, Inc. v. Hill*, 385 U.S. 374 (1967); *Cox Broadcasting Corp. v. Cohn*, 420 U.S. 469 (1975); *Florida Star v. B.J.F.*, 491 U.S. 524 (1989); C. von Hannover v. Germany, ECHR, 26/4/2004, Rec. 2004-VI 40 EHRR 1; Schwabe v. Austria, ECHR, 28/8/1992, A 242-B.

[75] See Ambrose 2012 and Sartor 2014.

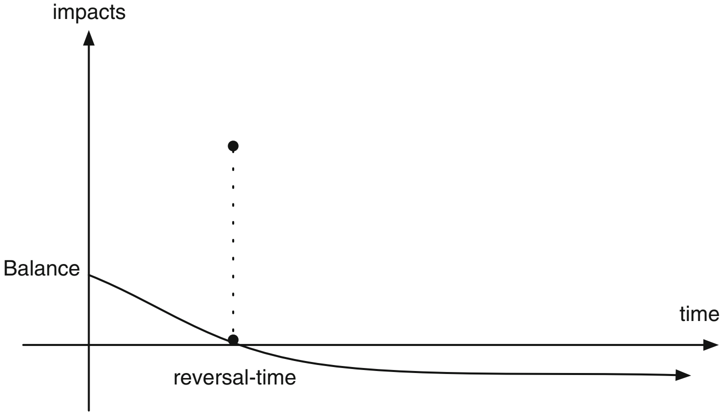


Fig. 7.2 Net social value of data processing over time

crimes or bankruptcies is distributed and remains accessible after such events took place.[76] This information is most relevant to the public for a short time after its publication because of its actuality, and then progressively loses its meaning and is used less, but continues to have a significant impact on the interests of the concerned person also because it may affect how that person is publicly perceived. In such cases, usually both impacts on freedom of expression and on privacy decrease as time goes by, but the diminution of the impact on freedom of expression proceeds at a quicker pace. Thus while at the beginning the benefit to the public would outweigh the loss to privacy, at a certain point in time, i.e., the reversal time, there is a change: the loss in privacy outweighs the benefit in freedom of expression. This is the point in time where, arguably, the data should be forgotten. In this typical context the pro-processing interests prevail over a RTBF up until a certain point in time, and after that point privacy takes the lead, as shown in Fig. 7.1.

Figure 7.2 clarifies this point by representing directly the difference between the differential advantage resulting from the favorable impact on publicity-interests (the publicity-related gain) and the differential disadvantage resulting from the unfavorable impact on privacy-interests (the privacy-related loss) obtained by processing the information. The balance is positive before the reversal-time, it is 0 at that point and then it becomes negative.

7.5.2 An Increase in Pro-processing Interests Over Time

The pro-processing interests are not always declining in time, because the benefits are not always immediate. Public interest in that which is newsworthy may be

[76] Cf. the Google Spain case referred to in section 3 (footnote 50).

fleeting, but public interest in history, social science, and cultural preservation last far longer. Think for instance of historical interests or when there is revived interest in the specifics of the content (e.g., an individual decides to run for office), as well as immediate interests met remotely when information is combined, aggregated, or reflected upon revealing previously unknown insights into the past or future.[77] The difficulty is that 'history' may be hard to recognize immediately, the interest very likely grows over time with regard to certain data subjects instead of declines.

However, we may be able to cope with such long-term interests in different ways. Because there is a significant difference between individuals like employers or first dates searching an individual and public interest, the meaning of the information in a context can differ; the employer is looking for a specific person while the public interest generally (not always) will be focused on a certain event in its context. Wikipedia's Biographies of Living Persons Policy draws a distinction between general public interest in the individual or the event or topic of an entry. It reads:

> Caution should be applied when identifying individuals who are discussed primarily in terms of a single event. When the name of a private individual has not been widely disseminated or has been intentionally concealed, such as in certain court cases or occupations, it is often preferable to omit it, especially when doing so does not result in a significant loss of context... Consider whether the inclusion of names of private living individuals who are not directly involved in an article's topic adds significant value.[78]

Based on this policy, the Star Wars Kid is not named in the entry on the Star Wars Kid.[79] Wikipedia also has a deletion policy that results in five thousand pages being deleted each day, one reasoning being a lack of 'notability,' which requires significant coverage, reliability, sources, independence from the subject, and a presumption that the subject is suitable for inclusion.[80] According to the policy, articles with unclear notability should not be deleted, but those that are clearly not notable should be and useful material preserved on the talk pages,[81] which are not indexed by Google.[82] Like Wikipedia, the right to be forgotten could (but does not) ask the difference between public interest and private searches in order to determine the right course of action when a user seeks to have personal information erased, as opposed to quick deletion or automatic public interest preservation. In some cases public interests may be served just as well by content that is anonymized (interference with the memory process on the level of encoding), as was done with the Star Wars Kid entry on Wikipedia. Moreover, preservation efforts could

[77] For further discussion of the information life cycle, *see* Ambrose *supra* note 6.

[78] "Wikipedia: Biographies of living persons – Wikipedia, the free encyclopedia," http://en.wikipedia.org/wiki/Wikipedia:Biographies_of_living_persons#Presumption_in_favor_of_privacy.

[79] "Talk: Star Wars Kid," Wikipedia, http://en.wikipedia.org/wiki/Talk:Star_Wars_Kid.

[80] "Wikipedia: Notability," Wikipedia, http://en.wikipedia.org/wiki/Wikipedia:Notability.

[81] Id.

[82] "Wikipedia talk: Talk pages not indexed by Google," Wikipedia, http://en.wikipedia.org/wiki/Wikipedia_talk:Talk_pages_not_indexed_by_Google.

seek to conserve that personal data that may continue to serve remote needs while offering limited search access where appropriate and in this way enabling a form of “forgetting” on the retrieval level.[83]

7.5.3 Carrots and Sticks

To determine how to regulate “digital forgetting”, it is not sufficient to consider the interests at stake. We also have to consider the motivations of the parties involved. Let us now focus on cases concerning the publication of publicly relevant information on online platforms.

A simplified representation is provided in the upper part of Fig. 7.3 where a linear relationship is assumed between the represented interests and time. In part A

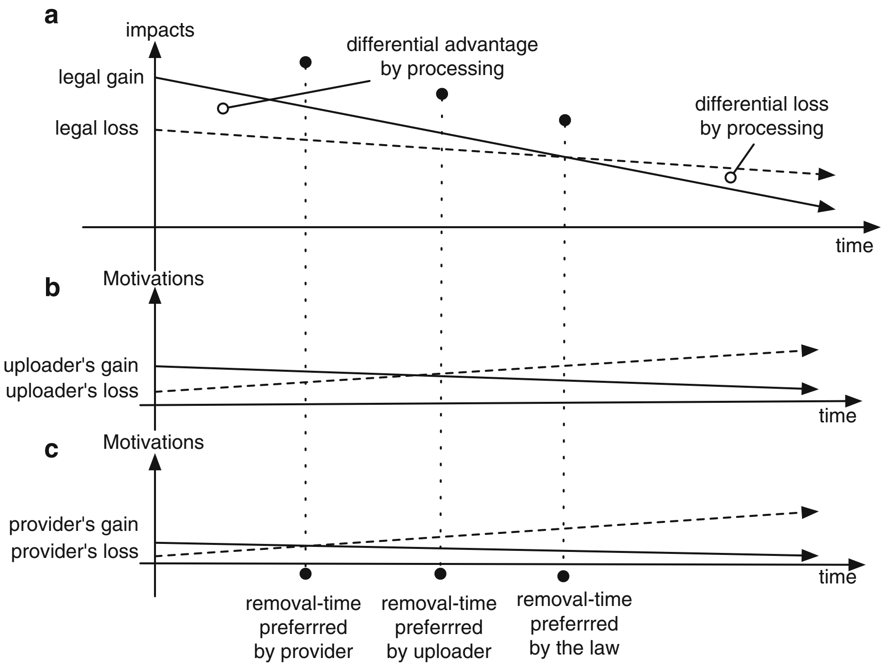


Fig. 7.3 Impacts of data processing related to interests over time

[83] For instance, the Internet Archive does not offer full-text search functionality on the site, but Google has performed a complete crawl of the site allowing the archive to be searched using Google’s “site:” feature. The Internet Archive also has detailed instructions for using robots.txt to prevent crawls and removal policy where the technical solution is not possible. “Removing Documents from the Wayback Machine,” Internet Archive, at http://archive.org/about/exclude.php.

of Fig. 7.3, the pro-processing curve starts at the higher level, but decreases more rapidly than the con-processing curve, so that at a switch point the two lines cross: from that point on, the damage to con-processing interests is no longer compensated by the benefit to pro-processing ones. Subsequently, processing provides a negative legal trade-off, which apparently justifies its impermissibility, and the provision of sanctions upon the processing parties, i.e., publisher/uploader of the information and the host provider who is storing it in his virtual repository (server/website/forum).

Figure 7.3 also contains a representation of the motivation uploader (part B) and of the host provider (part C), both of which are also decreasing, but remain positive (assuming that no sanctions are provided).

The meaning that data has for uploaders can differ and thus their motivation to upload. The uploader's motivation includes the economic gains the uploader expects from distributing the information (as is the case for newspapers and websites or host providers getting subscriptions or advertising), but also includes the moral and social importance one attributes to providing such information. Abstracting from different individual attitudes, we may assume that motivation for distributing information is measured by the maximum personal loss one would be ready to sustain for not distributing it, regardless of the grounds that explain this attitude.

Consider, for instance, the situation of a person who has to decide whether to upload on a blog information concerning a political or economic scandal, knowing that this may cause him some personal advantage (e.g., reputation, some chances of having a political role in the future, possible some financial gain resulting from the fact of attracting people to the blog) but larger personal losses (e.g., losing possible contracts, missing career advancements, even putting at risk one's life or freedom, etc.). Knowing also that this information would be highly beneficial to the public, contributing to curb the plight of corruption, while damaging the data subject, the motivation of such a person would likely be measured neither by the mere trade-off of personal gains and losses, nor by adding to this trade-off the full amount of the expected (net) public benefit. It would rather be measured by adding to the trade-off of personal gains and losses a quantity expressing the limited extent up to which the person internalizes the moral/social merit of his action, i.e., a quantity that indicates what additional personal loss he would be ready to sustain to accomplish that action.

Consider for instance a piece of news being published in an online journal, and assume that after a certain point in time the legal balance becomes negative. At that point in time, the publisher will still have an interest in keeping the news online, since it may still attract readers and thus produce revenue. Thus, if there were no law in place (abstracting from the possibility that the data subject uses private sanctions of incentives), the publisher would probably continue to distribute the information even when the legal trade-off has become negative.

The motivation is assumed to be similar to that of uploaders, while being generally lower, since providers host huge amounts of materials and have a small interest in continuing to distribute a specific single piece of information. Providers have a strong interest in having a legal discipline that does not make them liable for the distribution of illegal information. However, if the battle for a general exemption were lost, they would prefer to comply with removal requests, rather than be subject to sanctions in individual cases.

7.5.4 Sticks

We may assume that sanctions for failure to remove the data may include the compensation of the damage to the data subject, as requested by Art. 23 DPD. This compensation, according to national regulations, such as the Italian one, may also include non-economic damage. In addition, the sanctions may include administrative or criminal fines, as established by national legislation and required by the GDPR.

If such sanctions were always to be imposed upon a processing only after the point in time where the balance between pro- and con-processing interests is reversed, and the processing party knew exactly where this point is located, such a discipline would induce the behavior that maximizes the achievement of legal values. Before the reversal-time uploaders and providers would leave the material online, since they could enjoy the benefits resulting from the distribution of the information without encountering any legal sanction. After that point, they would take it down, since continuing to distribute the information would expose them to the obligation to compensate damages of the data subject, and to any further sanction established by data protection law.

This analysis however, does not consider that processing parties may be uncertain as to whether distributing certain information at a certain point in time provides a positive or a negative balance between publicity and privacy interests, being therefore lawful or rather unlawful. Or in any case, they may be uncertain as to how the competent decision maker will judge the issue. This uncertainty will very likely lead to premature withdrawal of the material by the parties involved in the distribution, i.e., at times when publicity interests still outweigh privacy interests. This anticipation will be larger when the uncertainty is greater or the motivation to distribute the material is smaller. If we assume, as it seems reasonable that uploaders have a stronger motivation to keep the material on line than providers, the expectation of a sanction will have a stronger anticipatory effect on providers than on uploaders, as Fig. 7.3 shows. Thus, uploaders and host providers would engage in premature self-censorship by honoring removal requests at times when the benefits of keeping the information on line still exceed the damage to the privacy interests of the concerned data subjects. Note that to have this effect the sanction does not need to be extremely severe: it suffices that the sanction, discounted by the probability of not being punished, overrides the motivation of the uploader. Also a punishment limited to damages (in particular when also moral damages are included) may have such a result. Hence, sanctioning the continued distribution from the point in time when the con-processing legal interests outweigh the pro-processing ones is likely to lead to anticipatory removal. Anticipatory removal would also happen when an unfulfilled request by the data subject was needed to trigger the sanction: anticipated requests would lead to anticipatory removals.

Consequently, a takedown system, where a user can simply request data be removed, requires the data controller to perform this assessment for themselves, which may lead to valuable information being removed, because there is so little guidance on how time should be incorporated into the removal equation.[84] While a RTBF that adheres to a life cycle approach is better than one that does not, data controllers may not be the appropriate source for establishing a standard for interpreting exceptions. In order for the RTBF to account for the interests of the data subject, the data controller, and the public, more guidance that recognizes the digital life cycle (ephemerality of digital content and public interest, as well as the value to remote and immediate users) would certainly bolster the legitimacy and strength of the RTBF.

7.6 Conclusion

In a world where you are what Google says you are and digital dossiers impact automated opportunities beyond view, the RTBF plays an important role in user participation. The complication is that information removal can be just as dangerous as information storage. Digital information sources, and especially the Web, function as very large external transactive memories. Acknowledging the growing wish of individuals to counter the 'remembering-by-default' of this memory requires the implementation of a form of digital 'forgetting'. However, because it is an external *transactive* memory, data controllers and data subjects are not the only parties to be considered, but also the interests of others: the public. Balancing these interests is difficult. We can, however, gain guidance and inspiration from the human memory process in which the factors 'meaning', 'use' and 'time' play important roles. 'Time' is a factor that generally supports 'forgetting' when the passed time increases, while 'meaning' and 'use' generally oppose forgetting when the meaning information and/or the frequency with which it is used increases. This makes 'time' a crucial element to acknowledge in relation to the RTBF. 'Meaning' and 'use' are often in some form or the other recognized by law as being important factors to retain data. For instance, the exceptions mentioned in art. 17 (3) GDPR, inter alia the freedom of expression, scientific and historical interests, are of such importance to the public that they oppose the 'forgetting' of the information.

However, beyond this general expression of the societal value of data retention in view of time, the exact role that time plays in current privacy or data protection law is not clear. Generally, 'time' can play two parts in law. On the one hand, 'time' can play a role as a weight in a balance of interests, as a factor adding or

[84] Ambrose 2013.

removing weight to the request to ‘forget’ personal information or its opposing interest, resulting in tipping the balance in either direction. On the other hand, ‘time’ can play a role as the marker of a discrete moment where the grounds for retention no longer hold and ‘forgetting’ of the data should follow.

In Sect. 7.4 the important points in time in data processing are identified, where time functions as a marker of a discrete moment in the information process. The identification of these points show that the ‘time’-cycle of data processing highly depends on the use of the data; the conditions under which the data are acquired, the purposes for which they are collected, and whether they are necessary. The analysis of the specific points in data processing shows the importance of the point in time with regard to the use of information in data processing for the invoking of a RTBF. Generally at the stages in the process where the information loses relevance for its use (at least for the initial purpose for which it was collected), the chance for a successful appeal on a RTBF is increased.

The role of time as a factor in a balance of interests is more complex. Important for this balancing is to recognize that information has a lifecycle and its value (also to the different interested parties) changes over time. Data is generally created to meet the current state of affairs in the world and has the most meaning and value in that context. The ‘newsworthiness’ of content is thus often fleeting, and information can easily become outdated, uncontextualized, and condensed or aggregated. Next to immediate needs, information can serve remote needs as it is combined, aggregated, or reflected upon revealing previously unknown insights into the past or future. Despite the fact that these information needs are important, there is very likely a point in time where the added value of personal data retention has diminished so far that the interests of the individual to be ‘forgotten’ prevail.

Utilizing time can help to inform appropriate decisions about the value of information. Because ‘time’ generally is an important force opposing memory processes and enabling forgetting, it should be of importance for the implementation of a right to be (digitally) forgotten. ‘Time’ could play a pivotal role, because at an operational level, it provides a tool for assessing the value of data or content, which is necessary in order to apply the exceptions and weigh rights and interests. However, the ‘time’ in relation to information life cycles will need to be researched more closely before it can be shaped into a usable tool. The role that times plays is very complex. A specific time span can mean something completely different for the data subject (lifetime perspective), the data controller (processing and use time) and for third parties (public interest, transactive memory use). The passing of 10 years in time has a different meaning in relation to the lifetime of an individual than it has in relation to historical interest of the public. The awareness of different time spans can tell us something about the time span that should be used for the implementation of the RTBF. Over the course of creation to storage to aggregation to edits to maintenance activity or death, digital data may serve or fail to meet immediate or remote needs. Both information needs are important and should be protected, but personal data at some point, may serve neither. This is the point in the information life cycle where a RTBF may be viable without triggering an exception. But how long and how little interest or use decreases the value of information enough to be overpowered by the interests of the data subject? And how does this time span relate to the lifetime of an individual? Many questions still remain to be answered, but what is clear is that approaching the RTBF from a time span that transcends the lifetime of a data subject defies its own use, because the rationale behind the RTBF is that individuals can achieve greater control of their (informational) *life*.

The changing role of time in this – already complex– balance of interests requires more specific research. Several issues will need to be explored like the balance between accountability and erasure and the balance between preservation and privacy. The point we stress in this paper is that we should not overlook or disregard the importance of 'time' when we are shaping policy mechanisms like the RTBF that aim to introduce 'forgetting' into data processing. Taking the passing of time into consideration can help assess the information landscape at issue for the RTBF and account for the changing values of information as it ages, establishing the balance all rights must find with other interests.

Acknowledgments This paper originates from the "Timing the Right to Be Forgotten" panel-discussion at the Computers, Privacy and Data Protection conference (CPDP) in Brussels 2014[85] organized by the Tilburg Institute for Law, Technology, and Society (TILT). We therefore would like to express our gratitude to TILT and CPDP for supporting and making this discussion possible. Paulan Korenhof her research is conducted within the Privacy and Identity Lab (PI.lab) and funded by SIDN.nl (http://www.sidn.nl).

References

Ambrose, M.L. (2012). It's about time: Privacy, information lifecycles, and the right to be forgotten. *Stanford Technology Law Review, 16*, 369–422.

Ambrose, M.L. (2013). Speaking of Forgetting: Analysis of Possible Non-EU Responses to the Right to be Forgotten and Speech Exception. In *TPRC 41: The 41st Research Conference on Communication, Information and Internet Policy*.

Ambrose, M. L., & Ausloos, J. (2013). The Right to be Forgotten Across the Pond. *Journal of Information Policy*, *3*.

Anderson, M., Eysenck, M.W., Baddeley, A. (2009). *Memory*, London: Psychology Press.

Andrade, De, N.N.G. (2012). Oblivion, the right to be different from oneself. Reproposing the right to be forgotten. *VII International Conference on Internet, Law & Politics. Net Neutrality and other challenges for the future of the Internet", IDP. Revista de Internet, Derecho y Política, 13*, 122–137.

Association of French Archivists (2013). The European Parliament: Adjourn the adoption of the regulation about personal data. Retrieved from https://www.change.org/petitions/the-european-parliament-adjourn-the-adoption-of-the-regulation-about-personal-data

Berg, Van den, B. & Leenes, R. (2010). Audience segregation in social network sites. *Social Computing (SocialCom), 2010 IEEE Second International Conference on Social Computing/Second IEEE International Conference on Privacy, Security, Risk and Trust). Minneapolis: IEEE*, 1111–1117.

[85] The video recording of the panel discussion and the presentations of the participants are available on the conference website, http://www.cpdpconferences.org/

Camenisch, J., Leenes, R.E. & Sommer, D. (Eds.), *Digital Privacy: PRIME – Privacy and Identity Management for Europe*. Heidelberg | Dordrecht: Springer.

Clark, A. (2003). *Natural-born cyborgs: Minds, technologies, and the future of human intelligence*, Oxford: Oxford University Press.

Draft Report (2012). 2012/0011 (COD). Retrieved from http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/pr/922/922387/922387en.pdf.

DuDai, Y. (2004). Memory from A to Z. Oxford: Oxford University Press (2004).

Edwards L., & E. Harbinja (2013). Protecting Post-Mortem Privacy: Reconsidering the Privacy Interests of the Deceased In A Digital World. *Cardozo Arts & Ent LJ*, *32*, 83–377.

Feeney, M. (Ed.) (1999). *The Digital Culture: Maximising the Nation's Investment* (A Synthesis of JISC/NPO Studies on the Preservation of Electronic Materials). London.

GDPR (2012). Proposal for a General Data Protection Regulation, COM(2012) 11 final, 25.1.2012. Retrieved from http://ec.europa.eu/justice/dataprotection/document/review2012/com_2012_11_en.pdf.

Gladney, H. M. (2007). *Preserving digital information* (pp. I-XXIII). Berlin: Springer.

Gomes, D. & Silva, M. J. (2006). Modelling Information Persistence on the Web, in Proceedings of the 6th International Conference on Web Engineering. ICWE'06.

Graux, H., Ausloos, J., & Valcke, P. (2012). The Right to Be Forgotten in the Internet Era. T*he Debate on Privacy and Security over the Network: Regulation and Markets*, 93–106.

Hadziselimovic, N., Vukojevic, V., Peter, F., Milnik, A., Fastenrath, M., Fenyves, B. G., ... & Stetak, A. (2014). Forgetting Is Regulated via Musashi-Mediated Translational Control of the Arp2/3 Complex. *Cell*, *156*(6), 1153–1166.

Harbinja, E. (2013). Does the EU data protection regime protect post-mortem privacy and what could be the potential alternatives? *SCRIPTed,* Vol. 10, Issue 1. Retrieved from http://script-ed.org/?p=843

Hill, D. G. (2009). *Data protection: Governance, risk management, and compliance*. CRC Press.

Husovec, M. (2014). ECtHR rules on liability of ISPs as a restriction of freedom of speech. *Journal of Intellectual Property Law & Practice*, *9*(2), 108–109.

Koehler, W. (2004). A longitudinal study of Web pages continued: a consideration of document persistence. *Information Research*, *9*(2).

Korenhof, P. (2014) Forgetting bits and pieces: an exploration of the "right to be forgotten" as implementation of "forgetting" in online memory processes. In *IFIP Advances in Information and Communication Technology series*, volume 0421. Springer.

MacLean, M., & Davis, B. H. (Eds.). (1998). *Time & bits: managing digital continuity*. Getty Publications.

Mayer-Schönberger, V. (2009). *Delete: The virtue of forgetting in the digital age*. Princeton: Princeton University Press.

Rosen, J. (2010). The web means the end of forgetting. *The New York Times, 21.*

Rosen, J. (2012). The right to be forgotten. *Stanford law review online*, *64*, 88.

Rosenzweig, R. (2011). *Clio Wired: The future of the past in the digital age*. Columbia University Press.

Sartor, G. (2014). The right to be forgotten: dynamics of privacy and publicity. In L. Floridi (Ed.), *The protection of information and the right to privacy*. Springer.

Schmidt, E. (2013). New Digital Age*, John Murray Publishers.*

Sparrow, B., Liu, J., & Wegner, D.M. (2011). Google effects on memory: Cognitive consequences of having information at our fingertips. *Science 333.6043*, 776–778.

Sutton, J. (2010). Memory. In: The Stanford Encyclopedia of Philosophy (Winter 2012 Edition), Edward N. Zalta (ed.), http://plato.stanford.edu/archives/win2012/entries/memory/ (last accessed 11 September 2014).

Szekely, I. (2012). The right to forget, the right to be forgotten; Personal reflections on the fate of personal data in the information society. In S. Gutwirth, R. Leenes, P. De Hert and Y. Poullet (Eds.), *European data protection: In good health?* (pp. 347–363). Dordrecht: Springer.

Vafopoulos, M. (2012). Being, space, and time on the web. *Metaphilosophy 43.4*, 405–425.

Weber, R. (2011). The Right to be Forgotten: More than a Pandora’s Box? In *2 JIPITEC 120*, 121. Retrieved from http://www.jipitec.eu/issues/jipitec-2-2-2011/3084/jipitec%202%20-%20a%20-%20weber.pdf.

Wegner, D.M. (1986). Transactive memory: A contemporary analysis of the group mind. In B. Mullen & G. R. Goethals (Eds.), *Theories of group behavior* (pp. 185–208). New York: Springer-Verlag.

Chapter 8
The '*Right to Be Forgotten*': Ten Reasons Why It Should Be Forgotten

Christiana Markou

Abstract This paper looks at the right to data erasure contained in Article 17 of the Draft Data Protection Regulation and challenges the choice to label it as a right 'to be forgotten'. It first explains what this right entails and why it is necessary particularly in the online world. It then puts forward ten reasons why its labeling as a 'right to be forgotten' does no good while it may cause harm. It shows that it does not tell the truth and is difficult to justify even if one is willing to think outside the strict boundaries of plain speech. It can mislead individuals as to its exact reach and as a result, unnecessarily trouble data controllers and eventually also frustrate the expectations of data subjects. The relevant label does not take into account the multi-purpose nature of the right (in a rapidly evolving online world), which necessitates a name that is both accurate and flexible. Fortunately, the 'to be forgotten' label can easily be omitted from the final text of the Regulation without necessitating any other change to the wording of Article 17. The right should simply be called a 'right to erasure', which cannot validly be subjected to similar objections. In general, the paper looks the right through the 'lens' of its label and offers an alternative introduction to the right and some of the issues pertaining to it.

8.1 Introduction

It is certainly not innovative to begin a piece on the now infamous 'right to be forgotten' by referring to Stacy Snyder. Miss Snyder is the young woman from the US who was denied a degree in education because of a picture she posted on MySpace, a social network website showing her wearing a pirate hat and drinking alcohol at a party. That picture was discovered by her supervisor and the Dean of the University, who thought that she did not deserve to be a teacher.[1] The story is

[1] Scott Michels, "Teachers' Virtual Lives Conflict With Classroom," *ABC News*, May 6, 2008, accessed October 8, 2013, http://abcnews.go.com/TheLaw/story?id=4791295&page=1.

C. Markou (✉)
European University Cyprus, Nicosia, Cyprus
e-mail: c.markou@euc.ac.cy

S. Gutwirth et al. (eds.), *Reforming European Data Protection Law*,
Law, Governance and Technology Series 20, DOI 10.1007/978-94-017-9385-8_8

very often mentioned in the literature on “the web that never forgets”[2] and on the so called ‘right to be forgotten’.[3] The first chapter of ‘Delete’, the book that has been described as “the most comprehensive discussion of the right to be forgotten in academic literature”[4] is named after the case of Miss Snyder.[5]

More generally, there has been an increasing tendency towards comparing the storage capabilities of the web with those of the human brain and emphasizing the fact that whereas human memory has limitations mirrored in human forgetfulness, the web “records everything and forgets nothing”.[6] The relevant line of thinking continues by pointing towards the usefulness of human forgetfulness[7] and calling for imputing the web with an analogous process, thereby correcting the ‘(un)forgetfulness’ deficiency of the web ‘brain’: “. . . the inability of computers to forget can at times be viewed as a bug, and not a feature”.[8] The introduction of a legal ‘right to be forgotten’ can be seen as an important step towards ‘fixing that bug’. By having a right to require erasure of their personal data on the web, individuals can in a way ‘force’ the web to forget it. Such legal right will in turn

[2] Jeffrey Rosen, “Free Speech, Privacy and the Web that Never Forgets”, *Journal of Telecommunications and High Technology Law*, 9 (2011), accessed October 8, 2013, http://www.jthtl.org/content/articles/V9I2/JTHTLv9i2_Rosen.PDF.

[3] See for example Pere SimónCastellano, “The Right to be Forgotten under European Law: a Constitutional debate”, *Lex Electronica*, 16.1 (2012): 7–8, accessed October 8, 2013, http://www.lex-electronica.org/docs/articles_300.pdf.

[4] Bert-JaapKoops, “Forgetting Footprints, Shunning Shadows: A Critical Analysis of the ‘Right to Be Forgotten’ in Big Data Practice”, *SCRIPTed*, 8(3), (2011): 233, accessed October 8, 2013, http://script-ed.org/wp-content/uploads/2011/12/koops.pdf.

[5] Viktor Mayer-Schönberger, *Delete: The Virtue of Forgetting in the Digital Age*, (New Jersey: Princeton University Press, 2011) 1.

[6] Jeffrey Rosen, “The Web Means the End of Forgetting”, *New York Times*, July 21, 2010, accessed October 8, 2013, http://www.nytimes.com/2010/07/25/magazine/25privacy-t2.html?pagewanted=all&_r=0. See for example, Pere SimónCastellano, “A Test for Data Protection Rights Effectiveness: Charting the Future of the ‘Right to be Forgotten’ Under European Law”, *The Columbia Journal of European Law Online*, (2013): 4–6, SSRN (AAT 2244352).

[7] Jean-Franois Blanchette and Deborah G. Johnson, Data Retention and the Panoptic Society: The Social Benefits of Forgetfulness”, *The Information Society*, 18 (2002): 36, accessed October 8, 2013, http://classes.dma.ucla.edu/Spring06/259M/readings/BlanchetteJohnson.pdf: “A world in which there is no forgetfulness—a world in which everything one does is recorded and never forgotten—is not a world conducive to the development of democratic citizens. It is a world in which one must hesitate over every act because every act has permanence, may be recalled and come back to haunt one, so to speak”; Hans Graux, Jef Ausloos and Peggy Valcke, “The Right to be Forgotten in the Internet Era”, *ICRI Research Paper No. 11*, (2012): 2–3, SSRN (AAT2174896); Kiyoshi Murata and Yohko Orito, “The Right to Forget/Be Forgotten”, *CEPE 2011*: Crossing Boundaries. Ethics in Interdisciplinary and Intercultural Relations, (2011): 193–197, accessed October 8, 2013, http://users.gw.utwente.nl/Coeckelbergh/site/publicaties/Conference%20Proceedings.pdf.

[8] Liam J. Bannon, “Forgetting as a Feature, not a Bug: the Duality of Memory and Implications for Ubiquitous Computing”, *CoDesign*, 2:1 (2006): 10, accessed October 8, 2013, http://archive.kmdi.utoronto.ca/events/documents/CODesign%20Forgetting.pdf.

encourage the development of 'technologies of erasure' (or of forgetfulness), the result ultimately being the technical introduction of forgetfulness into the 'brain' of the web.

It is not entirely clear if it is the 'human-web memory' analogy that inspired the labeling of this 'erasure' right in 'forgetfulness' terms or if it is the *vice versa*. The concept of a 'right to be forgotten' has appeared in the literature more than 20 years ago.[9] Also, as early as in the 1970s, Westin and Baker, talking about data erasure, referred to a choice to be made by society between "forgive-and-forget" and "preserve and evaluate".[10] Yet, online privacy and data protection were not very often discussed in terms of web *non-forgetfulness* in subsequent literature. It is therefore the recent re-surfacing of the concept of a 'right to be forgotten' by the European Commission[11] which must be the culprit behind this increasing emphasis on the need for the web to 'forget' comparably to how the human brain functions.

The 'forgotten' label however, may be fallible as may be the 'human-web memory' analogy that explains it. The fact that the case of Stacey Snyder has been epitomizing the particular right and its usefulness is similarly problematic. It may therefore be unsurprising that a right, which is not totally new, has provoked much controversy and criticism[12] mainly relating to its inconsistency with free speech[13] and the difficulties in its implementation.[14] This paper will first explain the basics of the right to be forgotten and acknowledge its importance in the online world where individuals constantly disclose personal data. Then it will explore the problems inherent in the chosen label through listing ten reasons why it is inappropriate. More specifically, it will arise that it does not make sense in plain speech in the particular context. Furthermore, the analogy it uses between web and human brain (or the way it uses it) is weak and cannot serve as an adequate explanation for the term. This is because contrary to the position inherent in the chosen label, the web may in many cases actually forget analogously to how the human brain

[9] Oscar H. Jr. Gandy, *The Panoptic sort: A political economy of personal information* (Boulder, CO: Westview Press) 285.

[10] Alan F. Westin and Michael A. Baker, *Databanks in a Free Society: Computers, Record-keeping, and Privacy* (New York: Quadrangle/New York Times, 1972), 268.

[11] European Commission, "A comprehensive approach on personal data protection in the European Union" (Communication) COM(2010) 609 final, 8.

[12] It has even been parallelized with "Pandora's Box", see Rolf H. Weber, "The Right to Be Forgotten: More Than a Pandora's Box?", *Journal of Intellectual Property, Information Technology and E-Commerce Law*, 2.2 (2011): 128, accessed October 8, 2013, http://www.jipitec.eu/issues/jipitec-2-2-2011/3084.

[13] See Paul A. Bernal, "A Right to Delete?", European Journal of Law and Technology, 2.2 (2011): 2–4, accessed October 8, 2013, http://ejlt.org//article/view/75/147; MugeFazlioglu, "Forget me not: the Clash of the Right to be Forgotten and Freedom of Expression on the Internet", International Data Privacy Law, 3.3 (2013): 153–155 who sees the criticisms valid; Jeffrey Rosen, supra n. 2; JefAusloos, "The 'Right to be Forgotten' – Worth Remembering?", *Computer Law and Security Review*, 28.2 (2012): 7–8, SSRN (ATT1970392).

[14] Fazlioglu, supra n. 13 pp. 151–152; Rosen, supra n. 2 p. 352; Ausloos, supra n. 13 p. 8.

does. Also, whereas the right provides for data erasure, human forgetting does not constitute data erasure from the brain in most cases. Apart from that, the particular label is both over-inclusive and under-inclusive, thus depicting a misleading picture of the actual reach of the right. The paper also rejects the alternative 'right to delete' label and concludes that the right should simply be referred to as a right to erasure. Thus, the compromise amendments recently voted by LIBE, the EU Parliamentary Committee on Civil Liberties, Justice and Home Affairs[15] which remove all references to a 'right to be forgotten' and rename the right to a 'right to erasure' should be welcomed and find representation in the final Regulation.

8.2 The Basics of the Right to Be Forgotten

In the Regulation as proposed by the Commission in 2012, the right appears in Article 17(1) which provides the following:

> The data subject shall have *the right to obtain from the controller the erasure of personal data relating to them and the abstention from further dissemination of such data*, especially in relation to personal data which are made available by the data subject while he or she was a child, where one of the following grounds applies: (a) the data are no longer necessary in relation to the purposes for which they were collected or otherwise processed; (b) the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or when the storage period consented to has expired, and where there is no other legal ground for the processing of the data; (c) the data subject objects to the processing of personal data pursuant to Article 19; (d) the processing of the data does not comply with this Regulation for other reasons.

Apart from having to erase personal data following a request by the data subject, the data controller must, under Article 17(2), "take all reasonable steps" to inform third parties who are processing any data made public by the controller "that a data subject requests them to erase any links to, or copy or replication of that personal data". Recognizing that it may be impossible to locate all such third parties, this additional obligation on the data controller is rightly limited to him making *reasonable attempts* to inform third parties. It is however a problem that third parties are not made subject to an obligation to satisfy any erasure requests.[16]

One can see that despite its somewhat 'mysterious' label, the right to be forgotten is essentially a right to have one's data erased. Such erasure right is not a total novelty. Since 1995 and the coming into being of the Data Protection

[15] 'Unofficial consolidated version of the LIBE Committee vote provided by the rapporteur', accessed January 11, 2014, http://www.janalbrecht.eu/fileadmin/material/Dokumente/DPR-Regulation-inofficial-consolidated-LIBE.pdf.

[16] For more on this issue, see infra pp. 17–18.

Directive (DPD),[17] individuals have had under Article 12(b) "the right to obtain from the controller… the rectification, *erasure* or blocking of data the processing of which does not comply with the provisions of this Directive, in particular because of the incomplete or inaccurate nature of the data".[18] Furthermore, the DPD, specifically Article 6(e) obliges data controllers to keep personal data "in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed". This obligation could be translated into a right vested on data subjects to have their data deleted or at least anonymized when its purposes have been fulfilled.[19] As regards the obligation to inform third parties in Article 17(2) of the Proposed Regulation, Article 12(c) of the DPD similarly provides that the data subject has the right to obtain from the data controller "notification to third parties to whom the data have been disclosed of any rectification, erasure or blocking carried out in compliance with (b), unless this proves impossible or involves a disproportionate effort".

These provisions of the DPD have been described as "diluted 'right to be forgotten' provisions"[20] and have been referred to as "means of enhancing control over one's own data" in a Communication published by the Commission in 2010.[21] It was actually in that context that the Commission first utilized the concept of 'a right to be forgotten' making it clear that it was not intended as anything dramatically new but simply as a clarification of the already existing 'data erasure' rights: "The Commission will… examine ways of… clarifying the so-called 'right to be forgotten', i.e. the right of individuals to have their data no longer processed and deleted when they are no longer needed for legitimate purposes".[22]

That the 'right to be forgotten' is essentially a *synonym* of the 'right to erasure' is reinforced in the Proposed Regulation published by the Commission 2 years later. Indeed, in Recital 53, the reference to the rights to rectification and erasure appearing in Article 12(b) of the DPD[23] are replaced by "…the right to have personal data…rectified and a 'right to be forgotten' where the retention of such data is not in compliance with this Regulation." Thus, the 'right to erasure' is replaced by the 'right to be forgotten', which is later in the Recital expanded upon in terms of data erasure. Rather confusingly, Article 17 of the Proposed Regulation

[17] 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.

[18] Emphasis added.

[19] A similar obligation is imposed on 'electronic communication service' providers in relation to traffic data by the Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector (the E-privacy Directive), Article 6.

[20] Ausloos, supra n. 13 p. 13.

[21] Supra n. 11.

[22] Ibid.

[23] See supra p. 5.

is titled as “Right to be forgotten *and* to erasure” suggesting that the two rights may be different. However, the actual provision is formulated only in ‘erasure’ terms containing no reference to the ‘forgotten’ word and rightly making commentators wonder: “could it be true that ‘the right to be forgotten’, as presented in the new EU proposed Regulation, does not in fact add much more than a ‘shiny’ title to Article 17”?[24]

Having said that the right to be forgotten is essentially a right to erasure, a look at Article 17(1) reveals that a main clarification (and sort of innovation) appears in paragraph (b), which renders the right exercisable on the ground of withdrawal of consent.[25] Whereas the consent of the data subject to data processing has always been a ground legitimizing that processing,[26] a right to withdraw previously-given consent does not expressly appear in the text of the DPD. As a result, the assertions of the Data Protection Working Party (DPWP) that it already exists implicitly[27] are unconvincing. Indeed, given that “personal data has become *the* currency on the Internet”[28] and the web default is that of data amassing, it may be naïve to expect that online businesses will readily comply with legal rules that *restrain* ‘personal data’ collection. It is noteworthy that the recently-amended legal provision on cookies, a notorious data-collecting technology, *explicitly* requires prior consumer consent to their use by websites.[29] Yet, it has met with strong resistance by online businesses, which, in many cases, continue to use cookies to collect data without securing consent.[30] One can imagine ‘the luck’ of rights and obligations that do not arise explicitly and are hidden ‘behind the lines’ of relevant laws.[31]

[24] Napoleon Xanthoulis, “Conceptualising a Right to Oblivion in the Digital World: A Human Rights-Based Approach”, SSRN (ATT 2064503): 17.

[25] See the text of the provision, supra at p. 4.

[26] See Data Protection Directive, Article 7(a).

[27] Article 29 Data Protection Working Party, ‘Opinion 15/2011 on the definition of consent’ WP187: 9, 32.

[28] Ausloos, supra n. 13 p. 2.

[29] The E-Privacy Directive (supra n. 19), Article 5(3).

[30] Christine Riefa and Christiana Markou, “Online Marketing: Advertisers Know You are a Dog on the Internet,” in Savin, A., Trzaskowski, J. (eds.) *Research Handbook on EU Internet Law* (Denmark: Edward Elgar 2014).

[31] This is also an argument against proposals mainly coming from US scholars to the effect that a legal right is inappropriate in this context and that technology alone should do the job (Rosen, supra n. 2 at p. 353). For additional reasons why “technology should have a serving function” and “cannot replace the legislator”, see Weber, supra n. 12 p. 127. Notably, technologists themselves who are certainly better aware of the capabilities and limitations of technology than lawyers conclude that “If there is to be an ambitious right to be forgotten, it must be a socio-legal construct, not a technical fix”, see Kieron O’Hara “Can Semantic Web Technology Help Implement a Right to be Forgotten?”, (paper presented at SCL 6th Annual Policy Forum on The New Shape of European Internet Regulation, September 11, 2011:4, accessed October 9, 2013, http://eprints.soton.ac.uk/273096/.

Unsurprisingly therefore, there have been initiatives emphasizing the absence of a right to revoke consent from the privacy-related legal regime and calling for the filling in of the relevant gap.[32] Article 7(3) of the Proposed Regulation, which explicitly provides for the right of individuals to withdraw consent coupled with Article 17(1)(b), which allows individuals to require erasure of data in relation to which they have withdrawn consent, may be seen as the Commission's response to these voices and should definitely be welcomed. Indeed, 'consent-as-*permanent*-permission' is not consistent with the ability to exercise meaningful control over one's own data. This is true especially given that "... individuals are ill-placed to make responsible decisions about their personal data given, on the one hand, well-documented cognitive biases, and on the other hand the increasing complexity of the information ecosystem."[33] Several decisions to give consent may therefore prove wrong, unintended and eventually be regretted. As a result, there has to be a way to reverse them (and also 'take back' any submitted data) so that individuals are not 'locked' in unwanted services and do not have to worry about whether a controller will indeed refrain from using it. As Fazlioglu acknowledges "The appeal of trading a phone number for a $5 coffee may in a sense be what the right to be forgotten seeks to shield us from".[34]

Another notable clarification is contained in Article 17(1)(c). Under Article 15 of the DPD, individuals already have the right to object to profiling, that is, the taking of automated decisions affecting them based on automated evaluations of, amongst others, their performance at work or reliability. Because of Article 17(1)(c) of the Proposed Regulation, they will also have the right to require that their data be erased and does not therefore remain in the possession of the data controller. That this enhances protection is indisputable. Individuals are best protected against the dangers of profiling and more generally, of any other data processing when data controllers have *no* data to process. Indeed, as Bernal states "Ultimately, wherever data exists, it is vulnerable – so the only way that data can really not be vulnerable is for it not to exist".[35]

[32] See for example, EnCoRe – Ensuring Consent and Revocation, http://www.encore-project.info/, accessed October 9, 2013.

[33] Omer Tene and Jules Polonetsky, "Privacy in the Age of Big Data: Time for Big Decisions", *Stanford Law Review Online*, 64 (2012) 67, accessed October 9, 2013, http://www.stanfordlawreview.org/online/privacy-paradox/big-data. For another discussion on why privacy choices are often fallible, see YoanHermstrüwer and Stephan Dickert, "Tearing the Veil of Privacy Law: An Experiment on Chilling Effects and the Right to Be Forgotten", Preprints of the Max Planck Institute for Research on Collective Goods Bonn 2013/15, p. 8, accessed October 9, 2013, http://www.coll.mpg.de/publications/3258.

[34] Supra n. 13 p. 156.

[35] Supra n. 13 p. 8.

More generally, by listing *specific* circumstances under which the right can be exercised, the Proposed Regulation breaks free from the possible objections against the current DPD right, which is exercisable solely on the vaguely-worded and perhaps inappropriately restrictive[36] ground that the data processing "does not comply with the provisions of this Directive, in particular because of the incomplete or inaccurate nature of the data".[37] By the same token, the newly-formulated right can be a handy way of exercising other important rights since by requesting erasure of his data, one effectively withdraws his consent under Article 7(3) of the Proposed Regulation or objects to profiling, thus exercising his right not be profiled conferred under Article 19.

It follows that EU officials are right to claim that the right to be forgotten clarifies and *strengthens* the existing 'erasure' right.[38] The fact that the EU legislator has paid attention to this right should also be applauded as erasure rights can greatly complement a consent-based data protection regime, thus bringing about better privacy.[39] Indeed, as data erasure means data extinction, Bernal is right to see in such rights the way to put individuals in control of data minimization and in effect, achieve a paradigm shift in privacy *away* from data amassing, which is the current default.[40] But did the right have to be called a 'right to be forgotten'? Indeed, it seems difficult to understand "[. . .] why it was necessary to create a new right under a new name".[41] The advantages of the new provision could be achieved (perhaps more successfully) by retaining the 'right to erasure' label and without resorting to the additional reference to a 'right to be forgotten', which is inappropriate for several reasons.

[36] This restriction may be caused by the particularization of the cases of incomplete or inaccurate data in Article 12(c) DPD.

[37] See Article 12(c) DPD, supra p. 5.

[38] European Commission, supra n. 11 p. 7, Viviane Reding, European Commission Speech 12/26, "The EU Data Protection Reform 2012: Making Europe the Standard Setter for Modern Data Protection Rules in the Digital Age" (speech given at Innovation Conference Digital, Life, Design, Munich, Germany, January 24, 2012), accessed October 9, 2013, http://europa.eu/rapid/press-release_SPEECH-12-26_en.htm.

[39] For more on how such rights can improve the privacy-related legal framework, see Ausloos, supra n. 13, pp. 6–7.

[40] Supra n. 13 p. 9.

[41] Christopher Kuner, "The European Commission's Proposed Data Protection Regulation: A Copernican Revolution in European Data Protection Law", *Privacy and Security Law Report*, 11 (2012): 11.

8.3 Ten Reasons Why the 'Forgotten' Label Should Be Forgotten

8.3.1 Reason One: The Exercise of the Right Does Not Cause One to Be Forgotten

There have been several proposals regarding the technical implementation of the right,[42] many of them basically enabling the disappearance or removal of personal information from the web. The simplest one, at least in cases such as where data is disclosed and/or processed with the consent of the data subject, would be a 'delete' button, which embodies the "manual ability to delete records"[43] proposed by Conley. As individuals can place information on the web (and 'in the hands' of online businesses) through mere clicks, they must be able to 'take it back' with comparable ease. This kind of implementation is obviously consistent with the very purpose of the right as a 'control-on-personal-data' enhancer.

The important question arising is the following: *If Miss Snyder could 'click and delete' the harmful picture from MySpace, would her supervisor and any other person who got to see it, forget about it?* The answer is negative of course. Human forgetting is a psychological process on which the subsequent removal of the picture can have little effect. As the supervisor would still remember what he saw, the picture did not just enter his short memory, which only lasts for 20–30 s.[44] It was transferred into his long term memory, which "can hold information over lengthy periods of time"[45] and even "the course of a life-span".[46] More generally, any harmful consequences normally arise very soon after the information has been viewed and therefore, before any question of forgetting it can naturally arise. Also, given the vastness of the web audience, information that goes online is probably bound to be viewed by somebody immediately. Anyone who gets to see it may pass it to others even if the information disappears from the web very soon after it has been posted. Indeed, the right is widely acknowledged as only operating *ex post*, that is, *after* the harm has occurred and thus, as only capable of preventing future or further harm.[47]

Therefore, if Miss Snyder could 'click and delete' the picture, thus exercising a 'right to be forgotten', *she would still not be forgotten*. Accordingly, the 'forgotten'

[42] Weber supra n. 12 pp. 126–127, Ausloos, supra n. 13 pp. 11–12, Koops, supra n. 4 pp. 248–249.

[43] Chris Conley, "The Right to Delete.", in *AAAI Spring Symposium: Intelligent Information Privacy Management* (AAAI Press, 2010), 57, accessed October 9, 2013, http://www.aaai.org/ocs/index.php/SSS/SSS10/paper/viewFile/1158./1482.

[44] "Psychology Class Notes Memory", AlleyDog.com, accessed October 9, 2013, http://www.alleydog.com/101notes/memory.html.

[45] Ibid.

[46] Ibid.

[47] Ausloos, supra n. 13 p. 9.

label of the right to erasure does not tell the truth. Moreover, while the benefit of preventing further harm is invaluable and should not be underestimated, that benefit is best reflected in a 'right not be seen' or 'not to be discovered' label, not a 'right to be forgotten' one.

8.3.2 Reason Two: You Cannot Sue One Because One Did Not Forget

Miss Snyder sued the university but failed in her action alleging a violation of her freedom of speech because her post was not considered protected speech.[48] Still, apart from the technical 'click and delete' implementation of the right, private legal action based on a violation of the right apparently comprises a powerful and also, logical mode of enforcement. This is true especially given that the right can be seen as an aspect of privacy, which is recognized as a human right in the EU, specifically by Article 8 of the European Convention of Human Rights and Article 7 of the Charter of Fundamental Rights of the EU.[49] Moreover, Article 77 of the Proposed Regulation confers on data subjects the right to claim compensation from data controllers or processors if they act in breach of the Regulation. Thus, Miss Snyder could sue MySpace on the ground that she was not given the opportunity to delete the picture or that she requested the website to erase the picture without success.

Yet again, the possibility of such private legal action does not render the chosen label sensible. Right on the contrary, since a psychological process, such as forgetting, cannot be forced or imposed and given also that one cannot *voluntarily* forget a piece of information,[50] no one can logically be sued for failing to forget.

[48] Rosen, supra n. 2 p. 346.

[49] See Xanthoulis, supra n. 24 p. 28. There are voices objecting to viewing the right as an aspect of privacy on the ground that privacy mainly relates to the protection of private information whereas the right to be forgotten extends to rendering publicly-known information private (Weber, supra n. 12 p. 122). Yet apart from the fact that privacy is now understood in a much broader sense (see Xanthoulis, pp. 22–23), the right to be forgotten is as an aspect of data protection, which is also a recognized human right in the EU contained in Article 8 of the Charter of Fundamental Rights of the EU, see Hans Graux, JefAusloos and Peggy Valcke, supra n. 7 p. 5. In any event, data protection is very closely related to privacy and other related rights. Andrade sees data protection as a procedural right that sets the methods or procedures through which substantive rights, be it privacy or identity ones, can be protected, see Norberto Nuno Gomes de Andrade, "Oblivion: The Right to Be Different from Oneself: Reproposing the Right to Be Forgotten", in *VII International Conference on Internet, Law & Politics. Net Neutrality and other challenges for the future of the Internet", IDP. Revista de Internet, Derecho y Política*, 13 (2012): 125.

[50] A sort of voluntary forgetting may take place in relation to certain traumatic events, see Kendra Cherry, "Explanations for Forgetting: Reasons Why We Forget", *About.com Psychology*, accessed October 9, 2013, http://psychology.about.com/od/cognitivepsychology/tp/explanations-for-forgetting.htm.

By the same token, no law can appropriately be formulated in terms that appear to prescribe that one *has to* forget whereas the 'forgotten' label does exactly this. Indeed, Xanthoulis writes that the right "… seems to take the perspective of third parties who are invited to take measures so as not to be able to remember/refer to certain aspects of an individual's past".[51] Other commentators also accuse the chosen label of "artificially re-creat(ing) a natural phenomenon".[52] This recreation will inevitably lead to lawsuits against parties on the ground that they omitted to forget, whereas parties can sensibly be sued on the ground of their failure to erase data, not their failure to forget.

8.3.3 Reason Three: The Right Cannot Retroactively Achieve the Results of Forgetfulness

One could argue that the word 'forgotten' is not intended to be given its ordinary meaning and that therefore, it is simply a parallelism or a metaphor based on the 'human-web memory' analogy. Koops indeed notes that the term "is not primarily meant psychologically (since forgetting is generally presented as a natural function of the human brain, which does not need reinforcement as such) but rather has social and legal implications: *the right not to be confronted with your past*…"[53] Admittedly, if the exercise of the right to be forgotten (or private action based on its violation) could correct *all* harms, the 'forgotten' label could be justified on the ground that the right can achieve the results of forgetfulness albeit retroactively. More specifically, the result of Miss Snyder having her degree eventually been awarded or being compensated for her losses would be *'as if'* Miss Snyder had been forgotten. Yet, a *total* restoration of damage is impossible. Even if Miss Snyder could recover some of her damage, she would still suffer some reputational harm at the very least. Her interest in not being confronted with that information cannot possibly fully be served. The right cannot therefore achieve retroactive forgetfulness, which could somewhat explain the chosen label.

8.3.4 Reason Four: 'Forgetting' Ordinarily Refers to Old or Outdated Data

The chosen label is also problematic because of the ordinary connotations of the 'forgotten' word regarding the *type* of information that is at stake. More specifically,

[51] Xanthoulis, supra n. 24 p. 9.

[52] Hans Graux, Jef Ausloos and Peggy Valcke, supra n. 7 p. 16.

[53] Supra n. 4, p. 231, emphasis added.

one normally expects *old* or *outdated* information to be forgotten. Apart from information that never makes it to one's long term memory,[54] information that is new, recent or just learned is not supposed to be forgotten. Thus, a right called a 'right to be forgotten' may be perceived as referring to outdated information such as past convictions or 'wild' university years. After all, the right has its roots in rights vested on ex-convicts to have the details of their convictions withdrawn from the public domain.[55] Such connotations were reinforced by Article 17(1) of the Proposed Regulation which specifically referred to information that one has disclosed while being a child[56] and are also mirrored in the various definitions of the right often found in the literature. As Koops confirms, "there seems to be a considerable common denominator in the literature about a "right to be forgotten", namely that someone has a significant interest (possibly to be protected in the form of a legal right) in not being confronted by others with elements of *her past*, more in particular with data from *the (more remote) past that are not relevant for present-day decisions or views about her*."[57]

Yet, the relevant right must be able to prove useful (also) in relation to information that is *not* old or outdated because "it is not only outdated data that can be detrimental to data subjects . . . "[58] Indeed, when online merchants or network advertising agencies process (clickstream) data derived from the browsing activity of individuals, they do *not* process outdated data. That data is normally recent and relevant to current personal circumstances, preferences and characteristics. Yet, individuals may have sufficient grounds for not wanting such businesses to process or even possess that information relating to them[59] and indeed, commentators have seen the right to be of particular usefulness in relation to such profiling/advertising data.[60] The same is true of social networking posts. The picture of Miss Snyder could *not* be regarded as outdated data *two days after it has been posted* for example. Yet, Miss Snyder could very well want to remove that picture on the ground that it was harming her identity by painting an untrue and damaging picture of her

[54] For example, telephone numbers which we learn in order to use them right away, see supra n. 44.

[55] Such rights are recognized by French and Italian law (see Bernal, supra n. p. 2; Lilian Mitrou and Maria Karyda, "EU's Data Protection Reform and the Right to be Forgotten - A Legal Response to a Technological Challenge?" (*paper presented at the 5th International Conference of Information Law and Ethics, Corfu, Greece, June 29–30, 2012*): 7, SSRN (ATT2165245), Swiss law (Weber, supra n. 12 p. 121; Franz Werro, "The Right to Inform v. the Right to be Forgotten: A Transatlantic Clash," in *Liability in the Third Millennium*, ed. Aurelia ColombiCiacchi, Christine Godt, Peter Rott and Leslie Jane Smith (Baden-Baden, F.R.G.: Nomos, 2009), 290–1) and some US State laws (Werro, p. 297 and Robert Kirk Walker, "The Right to Be Forgotten", *Hastings Law Journal*, 61 (2012): 272.

[56] LIBE has removed the relevant reference from Article 17(1) of the Draft Regulation, something that should be welcomed.

[57] Supra n. 4 p. 232 emphasis added.

[58] Koops, supra n. 4 p. 244.

[59] Infra p. 15.

[60] Hans Graux, JefAusloos and Peggy Valcke, supra n. 7 p. 14; Bernal, supra n. 13 p. 12.

character. As De Andrade explains, "... the right to personal identity concerns the correct image that one wants to project in society".[61] The particular commentator emphasizes the role of the right in protecting one's identity which can be harmed by de-contextualized data, that is, information or "... personal facts – whether truthful or not – which are capable of falsifying or transmitting a wrong image of one's identity".[62] Importantly however, such identity-harming information need *not* be information of *some age*. Sure enough, Miss Snyder would argue that the picture mirrored a de-contextualized, distorted and untruthful description of her character from the very moment it was taken and uploaded on MySpace. Indeed, there are moments in our life that are de-contextualized or identity-distorting *themselves*. The digital capture of such moments inevitably leads to data that is new, yet de-contextualized, which one may very well want to erase.

In this respect, the right to be forgotten should not be about the *age* of the data and fortunately, as already seen, Article 17(1) does *not* limit its reach to old or outdated data but extends it to any data in relation to which the data subject has withdrawn his consent. As Xanthoulis observes "most authors agree that a right to oblivion in the digital world aims in principle to grant an individual *control* not only of data related to unfortunate past events or the ability to prevent the publication of data in libel cases, *but in fact to all data in the digital world* ..."[63]

The fact that the right has nevertheless been labeled in terms of forgetfulness naturally tied to old and/or outdated data may cause problems. First of all, such misleadingly under-inclusive label[64] can lower the expectations of individuals regarding what they can achieve through its exercise, specifically by causing them to believe that they cannot utilize it in relation to data that has only recently been placed online. As a result, it can effectively reduce its practical relevance to old data, thus undermining its effectiveness.

Strikingly, the natural associations of the 'forgotten' term with *dated* information can also lead to the equally undesirable (opposite) result, namely over-inclusiveness.[65] More specifically, it can cause people to believe that they can get rid of their history, whether criminal, credit or otherwise, something which may

[61] De Andrade, supra n. 49 p. 125.

[62] Ibid at p. 127. American scholars seem to share this view despite the fact that they consider the right as sitting uneasily with American values such as the freedom of expression, see Karen Eltis, "Breaking Through the —Tower of Babel‖: A —Right to be Forgotten‖1 and How Trans-Systemic2 Thinking Can Help Re-Conceptualize Privacy Harm in the Age of Analytics", *Fordham* Intellectual *Property*, *Media* and *Entertainment Law Journal*, 22 (2011): 91: "... control over personal information is the power to control a measure of one‘s identity. This is indispensable to the —free unfolding of personality. It is also a right to a —rightful portrayal of self, crucial in the digital age ...".

[63] Xanthoulis, supra n. 24 p. 21, emphasis added.

[64] Hans Graux, Jef Ausloos and Peggy Valcke (supra n. 7 p. 14) also speak of 'under-inclusiveness' but in relation to the content of Article 17(2) and therefore, under a different light.

[65] Again Hans Graux, Jef Ausloos and Peggy Valcke (supra n. 7 p. 14) also speak of 'over-inclusiveness' but in relation to the content of Article 17(2).

be at odds with the freedom of speech[66] and generally, the public interest. Even though these interests can be safeguarded by the exceptions to the right laid down in Article 17(3) of the PDRP,[67] the numerous voices about a clash between the right to be forgotten and free speech serve as proof of the misleading over-inclusiveness of the label. Recall that an erasure right, which has *not* been called a 'right to be forgotten' exists since 1995 and has not attracted similar reactions. Though much of the literature on the relevant clash comes from Americans, who are notoriously free speech 'fanatics',[68] the EU commission also felt the need to publish on its website a "myth-busting"[69] document clarifying that "The right to be forgotten is not about rewriting history"[70] and reassuring that "The Commission's proposal protects freedom of expression and the freedom of the media, as well as historical and scientific research".[71] Such misunderstandings over the exact reach of the right can result in individuals 'bombarding' businesses with unfounded 'erasure' requests, thus placing an unnecessary burden on them and eventually also frustrate individual expectations. Moreover, as Bernal rightly points out, most of the Internet giants such as Google and Facebook are based in the 'free speech'-sensitive jurisdiction of the US. They are therefore likely to oppose the right, something which may have repercussions on its effectiveness all over the world.[72] Clearly therefore the 'forgotten' label may harm the right and undermine its effectiveness in multiple ways.

8.3.5 Reason Five: Forgetting Is Not Erasing

One may argue that Miss Snyder is the "icon of the problem of *digital* forgetting",[73] *not* of any issue relating to human forgetting and that therefore, the 'forgotten' label refers to individuals being forgotten *by the web*, not by human beings who happened to view published information. This possible explanation again mirrors the word 'forgotten' as deriving from the analogy between human and web brain.

[66] Bernal, supra n. 13 p. 2.

[67] For a discussion of these exceptions and how they protect historical records and free speech, see Bernal, supra n. 13 pp. 10–12. For a critique of these exceptions see Fazlioglu, spura n. 13 pp. 153–155.

[68] A prominent American law professor has stated the following: "So that's the American line: sexual surveillance by camera or possibly in blogs is possibly actionable, but very little else is, and I think that's a very good legal line to draw that respects free-speech values", Rosen, supra n. 2 p. 351.

[69] European Commission, "Myth-busting: what Commission proposals on data protection do and don't mean", Data Protection Newsroom, accessed October 9, 2013, http://ec.europa.eu/justice/newsroom/data-protection/news/121207_en.htm.

[70] Ibid.

[71] Ibid.

[72] Bernal, supra n. 13 p. 4.

[73] Rosen, supra n. 2 p. 345.

Undoubtedly, there are valid reasons why one would want to deprive the web of his data. MySpace, the website on which Stacey posted her picture, could not deny her a degree. Nor could it refuse her a job as several employers do on the basis of information about candidates found online.[74] Yet, it could classify Stacey as a member of a relevant group and on that basis, fill her online browsing experience with adverts and product offerings about 'kinky' underwear, for example. This commercial profiling and behavioural advertising can be privacy invasive and potentially damaging.[75] By deleting the picture, Stacey could assert a right not be profiled and/or not to be personally targeted (for advertising purposes) on its basis. Furthermore, the web is accessible to human beings. Because the web can retain data for long periods of time, human beings can have access to and utilize potentially damaging information that they would not otherwise know. Indeed, "computers can augment human capabilities . . . by 'supporting' our weak memory capabilities".[76] Thus, by erasing web information, Miss Snyder could assert a right not to be seen or discovered by others, such as employers, potential spouses or relatives. As one author writes "the "right to be forgotten" reflects the claim of an individual to have certain data deleted so that third persons can no longer trace them".[77]

However, the importance of the reasons why one may want the web not to retain her information does not sufficiently explain the labeling of the erasure of data as 'forgetting'. Forgetting does not necessarily mean that the initially-stored information has *disappeared* from our memory. "One of the most common causes of forgetting is the inability to retrieve information".[78] The information is there (and is available) but we have difficulty accessing it either because the information is old or because newer information interferes with older information. This difficulty can be overcome "if given enough time or cues".[79] It follows that even when a human being *forgets* a piece of information, that piece of information may still exist in her brain. By contrast, erasure, (which is what the right to be forgotten is all about), is a total removal of the information from the 'brain' of the web. Given that forgetting is not erasure, a right to erasure cannot accurately be called as a 'right to be forgotten'.

8.3.6 Reason Six: The Web Does Forget

Strikingly, the very analogy between human and web brain from which the 'forgotten' label has been inspired as well as the inherent thesis that the right will

[74] Rosen, supra n. 6.

[75] Riefa and Markou, supra n. 30.

[76] Bannon, supra n. 8 p. 9.

[77] Weber, supra n. 12 p. 120.

[78] Kendra Cherry, supra n. 50.

[79] Ibid.

furnish the web with the human-like forgetfulness *it lacks* may be challengeable. This is because at least some areas of the 'web brain' do function comparably to how the human brain does.

Indeed, old Facebook posts do *not* appear on newsfeeds. As time goes by and as more and more posts are published, older ones are pushed deep down in Facebook pages. As a result, one may need time and effort to locate an old post. Also Facebook posts cannot be located through search engines as in many cases they are accessible only to 'friends'. Similarly, recent news articles are shown on the homepage of online newspapers unlike dated ones which are hidden in one of those inner web pages that do not appear on screen unless one specifically searches for them, thus giving the website some cue. Even in relation to data about individual browsing behaviour stored and processed for behavioural advertising purposes, again older information seems to be 'buried' and 'forgotten' in favour of newly-recorded information. Indeed, it is likely that Amazon will display behavioural adverts that are relevant to the *recent* browsing activity of an individual, rather than individual preferences or interests expressed and recorded years ago for example.

Lievrouw also expresses the view that "...the idea of total, loss-free digital capture of all knowledge and information, or 'perfect remembering', should be viewed skeptically"[80]:

> The basic tools of the Internet (digital recording and transmission technologies, formats, and storage systems) are notably short lived and incompatible across platforms and standards, especially in comparison to physical and analog formats. Digital files and databases are notoriously fugitive and difficult to preserve in usable form for any extended period of time; they are among the most profoundly fragmented, disorganized, incompatible, and ephemeral forms of record-keeping ever devised... Robust, universal methods for the permanent preservation of digital records do not yet exist.[81]

Ambrose is far more specific. She refers to a whole line of study on information persistence that shows, amongst others, that only 15 % of online content remains available after a year.[82] She observes that this research has largely been overlooked by legal scholars[83] and casts serious doubt on the idea of permanence of online information.

If the web does *not* really lack 'forgetfulness' and if, as previously noted, data erasure is *not* 'forgetting', the analogy-based explanation of the relevant label obviously becomes weak, this comprising yet another reason why the chosen label is unfortunate.

[80] Leah A. Lievrouw, "The Next Decade in Internet Time: Ways ahead for new media studies", Information, Communication and Society, 15(5) (2012): 629.

[81] Ibid at pp. 629–630.

[82] Meg Leta Ambrose, "It is All About Time: Privacy, Information Cycles and the Right to be Forgotten", Stanford Technology Law Review, 16(2) (2013): 372–373.

[83] Ibid 371–372.

8.3.7 Reason Seven: The Right May Not Effectively Attack the Cause of Web Non-forgetfulness

The existence of search engines can powerfully challenge the validity of any arguments disputing the idea of 'web' perfect memory or non-forgetfulness. Indeed, these tools can easily unearth information that would otherwise be 'buried' and 'forgotten' in the 'deep waters' of the 'web ocean'. The several examples of individuals who had to bear the (negative) consequences of search results bringing to light embarrassing details of their past[84] cannot be ignored. In this respect, a right properly called a right 'to be forgotten' should strike against the very source of web non-forgetfulness, thus being exercisable against search engines. Interestingly however, an Attorney General of the Court of Justice of the EU (CJEU) had opined that Google was under no obligation to polish its search results in response to relevant erasure requests by individuals and that data subjects had to address their relevant requests to the websites publishing the information.[85]

This approach, though inconsistent with that taken by Spanish authorities,[86] has merit. Search engines are 'blind' indexes of what exists on the web and one should probably not want their content to be dictated by third parties; external interference with 'search engine' content should perhaps be tolerated only in certain (probably extreme) cases.[87] After all, when content is removed from the source, it will also probably disappear from Google search results at some point. Google also allows webmasters and individuals manually to remove from search results the cached copy of pages that have been updated or removed.[88]

Importantly however, a right *to be forgotten* that is not exercisable against the very cause of web *non-forgetfulness* could not suitably be called as such. The relevant Opinion of the Attorney General is based on the DPD, not the Draft Regulation, yet, both texts address the 'erasure' obligation to the data controller[89] whereas in the opinion of the Attorney General, search engines do not qualify as 'data controllers' when they list websites containing personal data of individuals.[90] Admittedly, following the compromise amendments voted by LIBE,[91] Article 17(1)

[84] For such examples, see Castellano, supra n. 3 p. 10.

[85] Case C-131/12, *Google Spain, Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González* (Opinion) 25 June 2013, para 138.

[86] For the Spanish approach, see Castellano supra n. 3 pp. 10–14.

[87] Google already allows for requests for deletion of certain information such as data exposing an individual to identity theft or sexually-explicit content, "Removal Policies", Google Inc., accessed October 9, 2013, https://support.google.com/websearch/answer/2744324.

[88] "Remove Information from Google", Google Inc, accessed February 26, 2014, https://support.google.com/websearch/troubleshooter/3111061?hl=en#ts=2889054,2889060.

[89] Article 12(b), DPD and Article 17(1), PDPR, emphasis added.

[90] Supra n. 85.

[91] Supra n. 15.

of the Draft Regulation additionally confers on data subjects the right "to obtain from third parties the erasure of any links to, or copy or replication of that data". As search engines would certainly qualify as 'third parties',[92] the said amendments remedy a significant deficiency of the initial Article 17(1)[93] and inevitably also invalidate this seventh reason why the 'forgotten' label is said to be unsuccessful.

Of course, this seventh reason is more directly invalidated by the long-awaited decision of the CJEU in the aforementioned Google Spain case. Disagreeing with the Attorney-General, the CJEU has found that search engines actually qualify as 'controllers' and that are also subject to an obligation to meet requests to remove links to pages containing (even true) personal data. This is so except where the interest of the general public to have access to that data overrides the conflicting interest of the data subject, something which would depend, for example, on whether the data subject has been a public figure.[94]

Yet, it remains to be seen whether this erasure obligation will have considerable practical effect. Search engines should be expected to resist this obligation to the extent that it goes beyond their already existing erasure policies. Indeed, Google warmly welcomed the aforementioned Opinion of the Attorney General as consistent with its views regarding freedom of expression and against censorship.[95] It is doubtful that these views will *easily* be sacrificed in the name of compliance with an EU legal rule which is viewed with some hesitation even by its very creators: "... both the Parliament and the Council agree that there are cases where the enforcement of the right to be forgotten is not realistic".[96] Moreover, the decision of the CJEU under the DPD, which contains no reference to a 'right to be forgotten', demonstrates that the purpose of the right can perfectly be achieved through a right simply called an 'erasure' right and reinforces the view that the 'forgotten' label is superfluous.

8.3.8 Reason Eight: Legal Rights Are No Places for Metaphors

One may insist that erasure causes inaccessibility to information and thus, some sort of (drastic) forgetting. As Blanchette and Johnson write, "When data are lost or

[92] See relevant definition in Article 2(f), DPD.

[93] See supra p. 4.

[94] Case C-131/12, *Google Spain, Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González,*13 May 2014, paras 32–41, 97, 98.

[95] Associated Press, "European Court of Justice lawyer sides with Google in 'right to be forgotten' case", *Fox News*, June 25, 2013, accessed January 11, 2014, http://www.foxnews.com/tech/2013/06/25/google-not-responsible-for-web-privacy/.

[96] Cedric Burton and Anna Pateraki, "Status of the Proposed EU Data Protection Regulation: Where Do We Stand?", *Privacy and Security Law Report*, 12 (2013): 1470, accessed January 11, 2014, http://www.wsgr.com/publications/PDFSearch/burton-090213.pdf, p. 3. On business resistance to the right, see also supra p. 12.

deleted, our behavior is forgotten . . . "[97] Along similar lines, Bannon states that "at one level, hitting the 'erase' button does cause the computer to forget".[98] Moreover, metaphors are not supposed to be exact (or totally accurate): "A man is not a fox, a family is not a house, a football is not a bomb, and the human brain is not a computer. Meaning generated by the metaphor process is always imperfect . . . Nor is there any way of reducing the potential for ambiguity and anomaly . . . by checking a metaphor against reality".[99]

It follows that if the word 'forgotten' is used metaphorically, the existence of certain differences between erasure and forgetting (such as the ones pinpointed earlier in this paper) does not render the relevant metaphor unsuccessful. It may be the case however that it is inappropriate to use metaphors as labels for legal rights.

In the AI field, the practice of imputing machines with human-like or cognitive attributes and as a result, referring to machines that 'learn', 'think' and 'know', is quite common and is said to assist scientists and researchers in studying and understanding machine behaviour.[100] Metaphors are not uncommon in the legal field either. Law has in fact been described as " . . . a magical world . . . where liens float, corporations reside, minds hold meetings, and promises run with the land".[101] Also, Sartor has spoken of "our natural tendency to attribute mental states to artificial systems, and to apply the consequent legal qualifications".[102] The right to be forgotten seems to mirror a similar tactic. Indeed, the (artificial) web has been attributed the mental or psychological state of non-forgetfulness which in turn led to and/or used to explain a legal right '*to be forgotten*'.

However, it is one thing to resort to such abstract thinking (or metaphors) to be helped in translating new technological phenomena into legal issues (or rules) and another to expressly incorporate any such metaphors in the very wording of the legal rules, especially of legal rights. Moreover, whereas metaphors are, in the legal field, used to render difficult-to-grasp phenomena more understandable, the choice of the 'forgotten' label strikingly seems to have involved the opposite. Indeed, what was at stake is something as concrete and understandable as 'data erasure', which has been described by reference to 'forgetting', a complicated and difficult-to-grasp psychological process!

Bernal rightly states that "One of the principle aims of rights in general is to put power into the hands of individuals . . . "[103] In effect, legal rights place the 'burden'

[97] Blanchette and Johnson, supra n. 7, p. 34.

[98] Bannon supra n. 8, p. 9.

[99] Richard H. Robbins, *The Belief Machine* (SUNY *Plattsburgh*, 1985), Chapter 2, accessed October 9, 2013, http://faculty.plattsburgh.edu/richard.robbins/belief/chapter_two.htm.

[100] Giovanni Sartor, "Cognitive Automata and the Law", *EUI Working Papers 2006/35*, SSRN (ATT963760), 67, 76.

[101] Bernard J. Hibbitts, "Making Sense of Metaphors", *Cardozo Law Review*, 16 (1994), accessed October 9, 2013, http://faculty.law.pitt.edu/hibbitts/meta_p1.htm.

[102] Sartor, supra n. 100, p. 67.

[103] Bernal, supra n. 13, p. 9.

of protection primarily on the shoulders of the right holders and indeed, the right to be forgotten has been said to incorporate the idea that the data subject is the “protector of his own data”.[104] Legal rights must therefore be labeled in a plain manner that requires no imagination and makes sense to the average right holder and his lawyer. Indeed, such (accurately-labeled) rights are likely to be invoked by right holders more frequently (i.e., not just in cases concerning outdated data) and under the right circumstances (i.e., not in order to extinct historical facts). The UK Information Commissioner makes this point perfectly: “It is essential that individuals understand the nature and extent of their rights, and that those rights are framed in a way that is not misleading to the individual. The “right to be forgotten” suggests possibilities that may not actually be available to the individual . . . ”[105]

8.3.9 Reason Nine: Multi-purpose Rights Necessitate Labels Describing Immediate Result

It must have arisen that the particular right can serve a variety of useful purposes and it could thus potentially be attached a variety of labels. Indeed, the preceding discussion has referred to a ‘right not to be profiled’, a ‘right not be targeted for advertising’ and a ‘right not be seen or discovered by others’. This reinforces the inappropriateness of the chosen label. Indeed, when a right can potentially achieve multiple ultimate purposes, choosing a name that cannot readily (or accurately) describe *any* of those purposes is probably unwise. In this respect, Weber is right to assert that “The concept is probably too vague to be successful”[106] adding that “ . . . a clearer picture of the actual objective of a new fundamental right is necessary”.[107] Indeed, under such circumstances, the wiser option is to go for an *all-purpose* label that only describes the immediate (and concrete) result of its exercise, which, in this context, is data erasure.

A ‘right to erasure’ label is acknowledged as “more accurate”[108] rightly. It is an open-ended concept regarding the ultimate purposes to be achieved and is therefore consistent with the ‘multi-function’ nature of the relevant right. With the rapid pace at which the Internet evolves, it is impossible to predict the new ways in which marketers and other parties will choose to deal with personal information. Similarly, governments will never cease to want to know as much as possible about individuals.

[104] Fazlioglu, supra n. 13 p. 152.

[105] Information Commissioner’s Office, “The Information Commissioner’s (United Kingdom) response to ‘A comprehensive approach on personal data protection in the European Union’”, January 14, 2011, accessed October 10, 2013, http://ec.europa.eu/justice/news/consulting_public/0006/contributions/public_authorities/ico_infocommoffice_en.pdf, p. 6.

[106] Supra n. 12 p. 128.

[107] Ibid.

[108] Hans Graux, Jef Ausloos and Peggy Valcke, supra n. 7 p. 16.

Accordingly, it is impossible to predict all the reasons why individuals might want to have their data erased. The 'right to erasure' label focus on the immediate result of data erasure, which it plainly describes and remains silent as to the ultimate purposes to be achieved through that erasure. As a result, it is wide enough to accommodate *all* possible reasons why one might want to exercise it, whether these are currently known or unknown. In this respect, it is a label that "does not, a priori, restrict the definitional scope of the concept, and therefore accommodates its potential future evolution and the broadening of the scope of the protected values".[109]

8.3.10 Reason Ten: It Is Easy to Get Rid of It

As already mentioned, Article 17 contains no reference to the 'forgotten' term which only appears in its title. This probably confirms that it offers nothing other than a bit of shine. Thus, its removal from the final text of the Regulation does not necessitate any re-wording of the particular provision and indeed, the version of the Draft Regulation published following the amendments voted by LIBE contains no sign of a 'right to be forgotten'.

8.4 Why Not a 'Right to Delete'?

Bernal, who also advocates the abandoning of the 'forgotten' label, proposes a 'right to delete' (as opposed to a right to erasure) which is "a direct right – a right to act".[110] Admittedly, this sounds more in line with the right as a tool allowing individuals to 'click and delete' certain personal information or otherwise, be in real control. Alternative modes of implementation which leave erasure to be performed by the data controller are criticized for being "tool(s) for controllers, not data subjects (who should be the beneficiaries of a right to be forgotten)".[111]

Importantly however, the very Article 17(1) may actually provide for 'a tool for controllers', as it is worded in terms of the data subject having "…the right *to obtain from the controller* the erasure of personal data relating to them".[112] Moreover, Article 17(3) provides that "*The controller* shall carry out the erasure without delay…"[113] Thus, a 'right to delete' would not be perfectly compatible with the wording of the provision and may lead to problems. More specifically, the

[109] Xanthoulis, supra n. 24 p. 9.

[110] Bernal, supra n. 13 p. 10.

[111] O'Hara supra n. 31 p. 3.

[112] PDPR, Article 17(1) emphasis added.

[113] PDPR, Article 17(3) emphasis added.

‘click and delete’ way of implementation of the right is appropriate in relation to information such as that which is uploaded on social media or recorded while an individual browses the internet. Even though these are the cases in relation to which there seems to be a consensus as to the usefulness of the right,[114] one can envisage additional situations to which the right may apply such as for example when one wants the erasure of an outdated article referring to him which has no historical value and is not of any interest to the public. In such cases and especially where the information at stake has not been uploaded by the data subject, it is only natural that she must address a relevant request to the controller. In this respect, the ‘the right to delete’ label may be over-inclusive causing the belief that the right renders the whole of the web ‘open to edit’ while in fact it does not purport to introduce a ‘delete’ button on every web page! It should be for the data protection authorities and/or the courts to construe the provision so as to require that (in appropriate cases) erasure be performable by the data subject, the controller having to make available the relevant erasure tool. Actually, such interpretation may be necessary given experiments that show that only few individuals may send erasure requests.[115] Given the large amounts of personal data left on a large number of websites, ‘request’ sending may be a real burden. As Hermstrüwer and Dickert observe, individuals may alternatively fear that by sending a request, they will share even more personal information with the data controller or draw attention to the information in relation to which they seek deletion.[116]

8.5 Conclusion

The choice of labeling the ‘erasure’ right of Article 17 as a ‘right to be forgotten’ has been unwise. The ‘right to erasure’, which already exists in the title of Article 17 describes the provision suitably and is not in any way problematic. This is unlike the ‘right to be forgotten’ label, which is unnecessary, confusing and even misleading for multiple reasons. Thus, the ‘right to be forgotten’ label should be forgotten and the recent LIBE compromise amendments which remove it should be mirrored in the final Regulation.[117]

An individual will not be forgotten by exercising the particular right and one cannot sensibly be sued for failing to forget certain information. As forgetting

[114] UK Information Commissioner, supra n. 104: “The ICUK can see some situations where the ‘right to be forgotten’ could work well in practice, such as where an individual wishes to delete their record from a social network, but these situations are limited”.

[115] Hermstrüwer and Dickert supra n. 33 p. 20.

[116] Ibid p. 23.

[117] The revised text of the Proposed Regulation publicized by the Council two months after the LIBE compromise amendments in the form of a Note from Presidency to the Working Party on Information Exchange and Data Protection is apparently based on the text prior to the LIBE

is a psychological process which cannot be achieved by erasing information, the 'forgotten' label, which appears to suggest the opposite is not logical. Furthermore, forgetfulness is often tied to old or outdated information, something which may cause the right to appear narrower and at the same time, wider than it really is. As a result, data subjects may not exercise it in all appropriate cases (such as when *recent* data is at stake) while they may exercise it in inappropriate ones (such as when historical or newsworthy data is involved). Moreover, contrary to what the particular label inherently suggests, forgetting does not normally mean erasure or total removal of information from memory. Additionally, the web may in fact forget something that threatens the validity of the very thesis on which the chosen label seems to have been founded, namely that the web never forgets and online information has permanence. Interestingly, even if the web does *not* forget, the 'forgotten' label makes little sense if the right cannot be exercised against what could be regarded as the very cause of web non-forgetfulness, namely search engines. Even though the CJEU has rendered the right exercisable against search engines, it has done so while interpreting the DPD which contains no reference to the 'forgotten' word. This reinforces the view that the particular label is unnecessary. Moreover, there is evidence to suggest that powerful commercial actors such as Google will resist an erasure obligation in any event.

Apart from the above, legal rights should not be labeled in abstract phrases (or metaphors), let alone in complex psychological terms, as they must be readily understandable to the average right holder whom they intend to empower. The 'erasure' right can achieve multiple purposes such as preventing profiling, targeting for advertising purposes and/or discovery of information by third parties. The appropriate label should not therefore emphasize one purpose while concealing another but must be able to accommodate all possible reasons why one may want to exercise the relevant right. By describing only the immediate (erasure) outcome of its exercise and remaining silent (and thus, 'open') as to the ultimate purposes to be achieved, the 'right to erasure' label seems to possess these qualities and is therefore, more appropriate than its 'forgotten' counterpart. Finally, it already exists in Article 17(1) of the Proposed Regulation and is perfectly compatible with its wording, unlike alternative labels such as the 'right to delete', which may also be misleading (or over-inclusive) and which would require substantive re-wording of the provision.

LIBE must have seen (at least some of) the reasons why the 'forgotten' label has been problematic, hence the removal of the particular label from the text of the Draft Regulation, which should definitely be welcomed. At the CPDP 2014, Walter Hötzendorfer of the University of Vienna told the author that the catchy 'forgotten' label has placed this important right under the spotlight and a lot of

amendments and still contains the 'right to be forgotten' label, see Council of the European Union, http://register.consilium.europa.eu/doc/srv?l=EN&t=PDF&gc=true&sc=false&f=ST%2017831%202013%20INIT&r=http%3A%2F%2Fregister.consilium.europa.eu%2Fpd%2Fen%2F13%2Fst17%2Fst17831.en13.pdf, accessed February 26, 2014.

people got to know about it as a result. It is very true that despite its many defects, the label may have served a (desirable) 'consumer awareness' role. As this purpose has probably been fulfilled now, the Article 17 right should be referred to as a right to erasure and the right *'to be forgotten'* should gradually be forgotten. All those who got to know about the existence of an important 'erasure' right, should now also get to know about its real nature and exact reach. This kind of knowledge is doubtless necessary if the right is to function as intended and successfully serve its very important purpose of placing individuals in better control of their personal data.

Chapter 9
Tracing the Right to Be Forgotten in the Short History of Data Protection Law: The "New Clothes" of an Old Right

Gabriela Zanfir

Abstract When the European Commission (EC) published its draft Data Protection Regulation (DPR) in early 2012, a swirl of concern hit data controllers regarding the introduction of a sophisticated "right to be forgotten" in the proposal for the future DPR, which was considered to unprecedentedly impact the internet and its economics. Critics and advocates of the right to be forgotten engaged in consistent theoretical debates, doubled by the technical discourse about its (un)feasibility. This paper "deconstructs" the right to be forgotten into the individual prerogatives which are in fact granted to persons. It shows that those prerogatives already exist to an extended degree in EU law, and have existed in the first data protection laws enforced in Europe. In addition, the controversial obligation to inform third parties about the erasure request is a "duty of best efforts" which pertains to controllers and which is significantly different than a duty to achieve a result. Recourse will be made to private law theory to underline this difference.

Keywords The right to be forgotten • Data protection • Privacy • Duty of best efforts

9.1 Setting the Scene – The Exponential Growth of the Digital Universe and Its Legal Consequences

It is impossible in general to remove data from the internet once it was published, according to a report released by the European Network and Information Security

This paper was submitted for publication before the author joined the EDPS. The opinions expressed in the paper pertain exclusively to the author and do not engage in any way the EDPS.

G. Zanfir (✉)
Legal Officer, European Data Protection Supervisor, Brussels, Belgium
e-mail: gabriela.zanfir@edps.europa.eu

S. Gutwirth et al. (eds.), *Reforming European Data Protection Law*,
Law, Governance and Technology Series 20, DOI 10.1007/978-94-017-9385-8_9

Agency.[1] This statement alone weakens the effectiveness of both existing and future privacy and data protection laws, as they fundamentally presuppose control of information and autonomy of the individual with regard to the informational self-determination.[2] One of the incurring problems brought by this fact is that, as Mayer-Schönberger explained, comprehensive digital memory makes it possible for our words and deeds to be judged not only by our present peers, but also by all our future ones.[3] This trans-temporal "judge" will have access to unimagined amount of data. In 2007, 2.4×10^{21} bits were stored by humanity in all of its technological devices, a figure which is approaching an order of magnitude of the roughly 10^{23} bits stored in the DNA of a human adult.[4] The estimated pace of growth of stored information in the digital universe is exponential: from 2005 to 2020, the digital universe will grow by a factor of 300, from 130 exabytes to 40,000 exabytes, or 40 trillion gigabytes.[5] This is only one of the reasons why legislators face great challenges.

The challenges are to become even greater, as it is predicted that the space-based web we currently have will gradually be replaced by a time-based worldstream, with all the information on the internet becoming a time-based structure – dynamic, always flowing, like time itself.[6] This mutation will impact even greater fundamental values such as privacy, and the legal instruments accorded to individuals must be proper and proportionate to the challenge. The development of Information Technology puts once again legislators in a sensitive position, similar to the one they faced in the late 1960s and early 1970s, after the appearance of the computer and the first computerized databases. Then, legislators found difficulties to regulate the emerging technology and the connected services, including massive data storage. Hondius wrote in 1975 that "[t]he first difficulty is their own and the public's unfamiliarity with computers and electronic data processing. It is this unfamiliarity, among other things, which prompted the demand for legislation. In the face of a

[1] *The right to be forgotten, between expectations and practice*, European Network and Information Security Agency, published on November 20, 2012, p. 13, accessed September 28, 2013, http://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/the-right-to-be-forgotten.

[2] See, for instance, Alan Westin, *Privacy and Freedom*, (New York: Atheneum, 1967); Louis Henkin, "Privacy and autonomy", *Columbia Law Review* 74 vol. 8 (1974); Antoinette Rouvroy and Yves Poullet, "The right to informational self-determination and the value of self-development: Reassessing the Importance of Privacy for Democracy", in *Reinventing Data Protection?*, ed. Serge Gutwirth et. al., 45–75. Springer Science + Business Media B.V. (2009).

[3] Viktor Mayer-Schönberger, *delete. The Virtue of Forgetting in the Digital Age*, (Princeton University Press, 2009), 11.

[4] Martin Hilbert and Priscila Lopez, "The World's Technological Capacity to Store, Communicate, and Compute Information", *Science* 332 (2011): 64. The authors showed that 94 % of the information stored in 1997 was digital.

[5] IDC, *The Digital Universe in 2020: Big Data, Bigger Digital Shadows, and Biggest Growth in the Far East* (2012), accessed September 28, 2013, http://www.emc.com/leadership/digital-universe/iview/executive-summary-a-universe-of.htm.

[6] David Gelernter "The End of the Web, Search, and Computer as We Know It", *Wired*, 1 February 2013. http://www.wired.com/opinion/2013/02/the-end-of-the-web-computers-and-search-as-we-know-it/ : accessed January 11, 2014.

powerful and ubiquitous computer, the public wanted a legal reassurance that this medium would not turn its unknown capacities against them. Governments were obliged to take this mood into account".[7]

Legislators in present time face similar challenges, only augmented by the ever-growing capacities of technology to store and process data. It is the development of internet what prompted the European Commission (EC) to start the reform process of the data protection regime existing in the European Union.[8] The declared purpose of the reform is to put individuals in control of their own data, while providing for strong enforcement of the data protection framework in the EU.[9] To this end, the draft proposal for a data protection regulation (DPR) enshrines a "right to be forgotten" in Article 17, according to which the person whose data are processed (the data subject) has the right to obtain from the controller the erasure of personal data relating to her, under certain conditions. The publication of the draft DPR generated responses such as the right to be forgotten "represents the biggest threat to free speech on the Internet in the coming decade".[10]

However, data subjects already had a right to ask for the deletion of processed personal information under Article 12 (b) of the Data Protection Directive (DPD),[11] which, if corroborated with the right to object to the processing of data, under Article 14 DPD, could amount to a right to be forgotten. In fact, the right to erasure as enshrined in the DPD merely aims at harmonizing the already existing provisions with regard to such a right in the first data protection laws enacted in Europe in the 1970s and 1980s.[12] The safeguard created in the 1970s for individuals and updated in 1995 in the DPD with regard to the deletion of their data from databases further developed in the complex "right to be forgotten", following the *design* of the regulated phenomenon itself.[13]

[7] Frits W. Hondius, *Emerging Data Protection in Europe* (Amsterdam: North-Holland Publishing Company; New York: American Elsevier Publishing Company, 1975), 82.

[8] See the press release of the European Commission from January 25, 2012, for the occasion of publishing the proposed reform package for data protection law in the European Union, accessed on September 30, 2013, http://europa.eu/rapid/press-release_IP-12-46_en.htm?locale=en.

[9] Explanatory Memorandum of the Proposal for a Regulation of the European Parliament and the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Brussels, January 25, 2012, COM(2012) 11 final, 2.

[10] Jeffrey Rosen, "The Right to be Forgotten", *64 Stanford Law Review Online 88* (2012).

[11] 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, 23/11/1995 P. 0031 – 0050.*

[12] Such as *Bundesdatenschutzgesetz* – the German Federal Law enforced in 1977, *Loi relatif a l'informatique, aux fichiers et aux libertes* – enforced in France in 1978, the *Data Protection Act*, adopted in 1984 by the British Parliament, *Wet Persoonsregistraties*, enforced in the Netherlands in 1989.

[13] Such a development can be deemed as being natural, if one would apply the Constructal law of systems, first to the digital universe and second to the law regulating the use of personal data in this system. See Adrian Bejan and Sylvie Lorente, "The constructal law of design and evolution in nature", *Philosophical Transactions of the Royal Society of London* 365 (2010): 1335–1347.

The draft DPR adds complexity to the content of the right, attempting to make it feasible in the current state of the digital environment by also imposing an *obligation de moyens* (duty of means) to controllers to make sure that the third parties that copied the targeted data acknowledge the deletion request. As it will be shown, not even this particular duty of means is all new in the European data protection law. This paper will decompose the right to be forgotten, as it is enshrined in the draft DPR, into tangible prerogatives, first by making a comprehensive analysis of its content (2). It will further analyze the duty of best efforts provided in the content of Article 17 DPR, showing why its execution is significantly different than the execution of a duty to achieve a result, with recourse to private law theory (3). Then, it will reveal why the content of the right to be forgotten is, in fact, old, by looking into the first data protection laws in Europe (4) and the current EU legislation (5). The conclusions will show that the right to be forgotten is the result of a natural evolution of an old right of the data subject (6).

9.2 A Closer Look upon the Content of the Right to Be Forgotten in the Draft DPR

9.2.1 The Right to Be Forgotten Does Not Mention Forgetting

The right to be forgotten, in conjunction with the clearer rules of jurisdiction with regard to processing data of citizens of the EU[14] are one of the reasons for which 2013 began with references to a US-EU "trade war"[15] originating in the data protection reform package.

Article 17 of the draft regulation, "the right to be forgotten and to erasure", is one of the most complex provisions in the DPR proposal, being expanded in the original version of the draft DPR on over 9 paragraphs.[16]

[14] The Future of Privacy Forum observed in a White Paper that "this extension of extraterritorial application [See Article 3(2) DPR – n.n.] constitutes a dramatic shift from a country of origin to a country of destination approach, and portends general application of the GDPR to the entire Internet"; Omer Tene and Christopher Wolf, *Overextended: Jurisdiction and Applicable Law under the EU General Data Protection Regulation* White Paper (2013). Available on http://www.futureofprivacy.org/wp-content/uploads/FINAL-Future-of-Privacy-Forum-White-Paper-on-Jurisdiction-and-Applicable-Law-January-20134.pdf, last accessed on 11 January 2014.

[15] Cyrus Farivar, "Proposed EU data protection reform could start a trade war, US official says", ArsTechnica, 1 February, 2013, http://arstechnica.com/tech-policy/2013/01/proposed-eu-data-protection-reform-could-start-a-trade-war-us-official-says/, accessed on 11 January 2014.

[16] The first paragraph states that: *The data subject shall have the right to obtain from the controller the erasure of personal data relating to them and the abstention from further dissemination of such data, especially in relation to personal data which are made available by the data subject while he or she was a child, where one of the following grounds applies: (a) the data are no longer necessary in relation to the purposes for which they were collected or otherwise processed; (b) the data subject withdraws consent on which the processing is based according to point (a) of*

The first observation regarding the content of Article 17 of the draft DPR is that the provision itself does not mention the word "forget" or any of its derivates, but it refers to "erasure" and "abstention from further dissemination".

Moreover, the Civil Liberties Committee of the European Parliament,[17] following the Report by Jan Philipp Albrecht[18] – the Rapporteur MEP for the DPR proposal, changed the title of Article 17 into "Right to erasure", in the context of the vote on its final position concerning the DPR proposal. This form of the proposal was kept in the final version adopted in March 2014 by the plenary of the European Parliament (EP). Thus, the EP will engage in negotiations with the Council for the final text of the regulation with a "right to erasure" mandate. In fact, 'right to be forgotten' was already considered in the literature to be an "emotive and misleading label"[19]; by renaming it 'right to erasure', "the emphasis would be on data rather than stories",[20] which would probably contribute to a less aggressive freedom of speech discourse against its enforcement.

While the concepts of "erasure of data" and "abstention for further dissemination" put together can be confusing, as erased data could not physically be disseminated, they do make sense in the digital processing of data, where the possibility to definitively erase information is still under debate.[21]

In an attempt to avoid this confusion, the Working Party on Information Exchange and Data Protection of the European Council (WP IEDP), in a revised version of the draft DPR, erased the "abstention" provision from Article 17 and created Article 17a, "the right to restriction of processing", according to which

Article 6(1), or when the storage period consented to has expired, and where there is no other legal ground for the processing of the data; (c) the data subject objects to the processing of personal data pursuant to Article 19; (d) the processing of the data does not comply with this Regulation for other reasons. {The Civil Liberties Committee of the European Parliament added a point (ca) to Article 17(1) of the DPR proposal – "a court or regulatory authority based in the Union has ruled as final and absolute that the data concerned must be erased". As well, The Working Party on Information Exchange and Data Protection of the European Council, during the process of negotiations on the DPR text, and according to a revised version of the DPR published on 21 June 2013, inserted in the draft proposal a point (e), which states that the data also have to be erased "for compliance with a legal obligation to which the controller is subject" [Council of the European Union, Interinstitutional File 2012/0011 (COD); 11013/13]}.

[17] The Civil Liberties, Justice and Home Affairs Committee (LIBE) of the European Parliament adopted on 21 October 2013 the compromise amendments to the DPR proposal. The text resulted from the LIBE vote will be further used in this paper as "the LIBE text".

[18] LIBE Committee – Rapporteur Jan Philipp Albrecht, Draft Report on the 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 (COM(2012)011 – C7-0025/2012 – 2012/0011(COD)), 16.1.2013.

[19] Paul Bernal, "The EU, the US and Right to be Forgotten", in *Reloading Data Protection. Multidisciplinary Insights and Contemporary Challenges,* eds. S. Gutwirth, R. Leenes, P. de Hert, (Dordrecht, Heidelberg, London, New York: Springer, 2014), 75.

[20] Id., at 76.

[21] See, for instance, James Wardwell and Stevenson G. Smith "Recovering erased digital evidence from CD-RW disk in a child exploitation investigation", *Digital Investigation* Vol. 5, 1–2 (2008): 6–9.

the data subject has the right "to obtain from the controller the restriction of the processing of personal data" for short term, if the accuracy of the data is contested or the data subject exercised the right to object to the data processing – until the requests are considered, or for a longer term, if the controller no longer needs the personal data, but they are required by the data subject for the establishment, exercise or defense of legal claims.[22] By restriction of processing, WP IEDP means that the data "may, with the exception of storage, only be processed with the data subject's consent or for the establishment, exercise or defence of legal claims or for the protection of the rights of another natural or legal person or for reasons of important public interest" (Article 17a(3)). It should be mentioned that the LIBE text does not contain further clarification on this matter.

The second observation regarding Article 17 of the draft DPR is that the provision is highly technical, without making any references to the fundaments of a right to be forgotten, merely proposing an instrument which would give effect to any of such possible fundaments. In this regard, Koops has identified three guises of the right to be forgotten that are featured in the literature: a right to have data deleted in due time, a claim on a clean slate, and the right to unrestrained individual expression here and now.[23] In another opinion regarding the fundaments of the right enshrined in Article 17 of the DPR proposal, it was stated that "as currently framed, the European right to be forgotten may be viewed as affording protection for one's reputation rather than privacy"[24] – which resembles the "claim on a clean slate" fundament. A better fitting approach to the procedural characteristic previously underlined is that even though the right to be forgotten "may be conceived as a legal right, *de lege lata*, it can also be seen as a value or interest worthy of protection or a policy goal to be achieved by some means or other, whether through law or through other regulatory mechanism",[25] meaning that it can be used to protect any of the personality rights of the data subject – privacy, dignity and so forth.

The third observation is that Article 17(1) of the DPR proposal does not refer to inaccurate data, but clearly links the quality of the data to be erased to the purpose limitation principle. Hence, all the data which are no longer necessary in relation to the purposes for which they were collected or processed must be erased, on the request of the data subject.

The fourth observation is that the new provision makes a clear link between the right to object and the right to erasure, by stating that erasure may be obtained when the data subject objects to the processing of personal data pursuant to Article 19 (the right to object). The WP IEDP added to point (c) of Article 17(1) DPR that

[22] The Working Party on Information Exchange and Data Protection (n 16), 97.

[23] Bert-Jaap Koops, 'Forgetting Footprints, Shunning Shadows. A Critical Analysis of the "Right to be Forgotten" in Big Data Practice', *Tilburg Law School Legal Studies Research Paper Series* 8 (2012) at 8.

[24] Omer Tene and Jules Polonetsky 'Judged by the Tin Man: Individual Rights in the Age of Big Data', *Journal of Telecommunications and High Technology Law*, forthcoming, available at SSRN http://ssrn.com/abstract=2311040, last accessed on 11 January 2014. (2013): 14.

[25] Id. at 3.

the data should be erased in this situation only if "there are no overriding legitimate grounds for the processing or the data subject objects to the processing of personal data pursuant to Article 19(2)". As the effect of the right to object is not necessarily the erasure of data, in order to obtain it, the data subject, apparently, must make a specific request in this regard, alongside with her objection.

Last, the right to erasure becomes effective when the processing of data does not comply with the proposed regulation "for other reasons", which could mean, for instance, that their processing is not based on any of the six legal grounds for processing or that the principles of fair processing, and the rules regarding the security of data are not observed.

9.2.2 Freedom of Expression, an Express Exception of the Right to Be Forgotten

According to Article 17(3) of the DPR proposal, the primary exception for the right to erasure is freedom of expression. It is expected that the clash between freedom of expression and the right to be forgotten, in conjunction with the overextended jurisdiction of the data protection provisions, will generate overriding problems in the application of the future DPR. The key issue in this matter appears not to be the fundamentally different conception of privacy in the US and EU,[26] but the fundamentally different understanding of the right to free speech and its limitations. McNealy explained that it is difficult, if not virtually impossible, for American courts, at the current state of the development of the newsworthiness exception in US tort law regarding the protection of privacy, to admit requests for a right to erase private information made public.[27]

On the contrary, in the European culture of the protection of fundamental rights, the courts – national or supranational, always strike a balance between two conflicting rights and decide on the merits of each particular case,[28] taking into account the principle of proportionality or pivoting around the concept of human dignity.[29]

[26] See, for instance, James Q. Whitman, "The Two Western Cultures of Privacy: Dignity Versus Liberty", *Yale Law Journal 113* (2004); Robert Kirk Walker, "The Right to be Forgotten", *Hastings Law Journal 64* (2012): 101–129.

[27] Jasmine E. McNealy, "The emerging conflict between newsworthiness and the right to be forgotten", *Northern Kentucky Law Review*, *vol. 39:2* (2012): 119–135; 'The law of public disclosure of private facts precludes recovery where the published private information is not of "legitimate public concern." However, the Restatement offers that the publication *is* subject to First Amendment protection if the defendant can show that the information is of public concern. Although "of public concern" would obviously anticipate news, it also includes entertainment, film, books, and most anything that stops short of a morbid fascination' (at 126).

[28] See the famous case Von Hanover v. Germany, Application No. 59320/2000, European Court of Human Rights.

[29] See, in general, Gert Brüggemeier, Aurora Colombi Ciacchi and Peter O'Callaghan, *Personality Rights in European Tort Law*, (New York: Cambridge University Press, 2010).

The "balance of rights" approach in the tension of the right to be forgotten and freedom of expression is even more encouraged by the recognition of the fundamental right to the protection of personal data in Article 8 of the European Charter of Fundamental Rights of the EU (the Charter), which entered into force in 2009, as it places data protection in the realm of fundamental rights, where proportionality and necessity have a *sine qua non* status in the exercise of rights. Article 52(2) of the Charter itself states that limitations to the rights it provides for are "subject to the principle of proportionality" and "may be made only if they are necessary and genuinely meet objectives of general interest recognized by the Union or *need to protect the rights and freedoms of others*" (emphasis of the author). Moreover, Article 54 of the Charter prohibits "the abuse of rights", providing that "nothing in this Charter shall be interpreted as implying any right to engage in any activity or to perform any act aimed at the destruction of any of the rights and freedoms recognized in this Charter or at their limitation to a greater extent than is provided therein." Therefore, the right to the protection of personal data must not be interpreted as aiming to disregard or to limit to an extensive degree the right to freedom of expression or information (Article 11 of the Charter), freedom of thought (Article 10), or even freedom to conduct a business (Article 16).

In this regard, the Court of Justice of the European Union already underlined in its *Schecke* judgment that "the right to the protection of personal data is not, however, an absolute right, but must be considered *in relation to its function in society*"[30] (emphasis of the author). The Court added that "the limitations which may lawfully be imposed on the right to the protection of personal data correspond to those tolerated in relation to Article 8 of the Convention",[31] paving thus the way for the case-law of the European Court of Human Rights under Article 8 of the Convention to be taken into account whenever at least one other right will counterbalance the right to personal data protection.

As for the *locus standi* of the right to ask the erasure of data within the right to personal data protection, it was previously argued that, similar to the other 'rights of the data subject', it represents a prerogative of the substantive right to personal data protection.[32]

AG Jääskinen considered that "this fundamental right (to personal data protection – n.n.), being a restatement of the European Union and Council of Europe *acquis* in this field, emphasizes the importance of protection of personal data, but it does not as such add any significant new elements to the interpretation of the

[30] Court of Justice of the European Union, Decision of the Court in Joined Cases C-92/09 and C-93/09 *Volker und Markus Schecke and Eifert* [2010], ECR I-11063, para. 48.

[31] Id., para. 52.

[32] Gabriela Zanfir, "Forgetting about consent. Why the focus should be on suitable safeguards in data protection law" in *Reloading Data Protection. Multidisciplinary Insights and Contemporary Challenges,* eds. S. Gutwirth, R. Leenes, P. de Hert, (Dordrecht, Heidelberg, London, New York: Springer, 2014), 246.

Directive (95/46 – n.n.)".[33] A similar point of view was taken by AG Sharpston, with regard to the right to access personal data, when she argued that Article 8 of the Charter "does not articulate a separate standard governing the form in which access must be made available"[34] than the one established by Article 12 DPD. Therefore, the exercise of the right to be forgotten, or the right to erasure, applied in the context of a fundamental rights "dispute", will be guided by the provisions of the secondary legislation regarding personal data protection. In this context, it is without doubt that the Data Protection Directive, which will be replaced by the DPR, contains "conditions and limitations for the exercise of the right to the protection of personal data".[35]

However, as it was already underlined in the literature, in practice it might prove to be difficult for data controllers to make decisions which imply assessing to what extent the request for erasure of data falls under any of the exceptions of the right to be forgotten.[36] Indeed, pragmatic and swift support from national data protection authorities might alleviate these issues to some extent.[37] The national courts will also have an important part in striking the balance between the right to be forgotten and the other rights or values.

9.3 The Duty of Best Efforts (*Obligation de moyens*) Correlative to the Proposed Right to Be Forgotten

Article 17(2) is the provision which generated much of the discussions surrounding the right to be forgotten, because it entails an obligation of the controller "to take all reasonable steps, including technical measures, in relation to data for the publication of which the controller is responsible, to inform third parties which are processing such data, that a data subject requests them to erase any links to, or copy or replication of that personal data". The provision makes it clear that a controller is considered responsible for the publication of data "where the controller has authorized a third party publication".

[33] Opinion of Advocate General Jääskinen delivered on 25 June 2013 in Case C-131/12 *Google Spain* vs. *Agencia Espanola de Proteccion de Datos*, para. 113.

[34] Opinion of Advocate General Sharpston delivered on 12 December 2013 in Joined Cases C-141/12 and C-372/12, *Y.S. v. Minister voor Immigratie* and *Minister voor Immigratie v. M. and S.*, para. 70.

[35] *Explanation relating to the Charter of Fundamental Rights,* 2007/C 303/02, OJ 303/17, 14.12.2007 – explanation of Article 8.

[36] Meg Leta Ambrose and Jef Ausloos, "The right to be forgotten across the pond", Telecommunications Policy Research Conference (2012), available on http://ssrn.com/abstract=2032325, last accessed on 11 January 2014. at 7.

[37] Ibid.

The distinction between the duty to achieve a specific result (*obligation de resultat*) and the duty of best efforts (*obligation de moyens*) is a matter of Contract law and is mostly used in civil law systems, in particular under French law. Nevertheless, an echo of this distinction can be found in some international and EU texts.[38] A comparison between Contract law obligations and the provisions of the DPR proposal, even though unnatural due to the private law/public law dichotomy, can prove to be useful in the terms of establishing the situation in which a controller can be held liable for not complying with the provisions enshrined in Article 17(2) of the DPR proposal. This provision is construed as a duty of best efforts.

According to Article 5.1.4 of the UNIDROIT Principles,[39] in the presence of a duty to achieve a specific result, the party "is bound to achieve that result", whereas in the presence of a duty of best efforts in the performance of an activity, the party "is bound to make such efforts as would be made by a reasonable person of the same kind in the same circumstances". This distinction is very important because the degree of diligence required of a party in the performance of an obligation varies considerably depending upon the nature of the obligation incurred.[40]

The assessment of non-performance of an obligation of best efforts calls for a less severe judgment, based on a comparison with the efforts a reasonable person of the same kind would have made in similar circumstances.[41] In other words, if the debtor was obliged to fulfill an *obligation de resultat*, it falls on the *obligée* only to prove that the result owed was not achieved. If the debtor however was only obliged to fulfill an *obligation de moyens*, the *obligée* has to prove that the debtor *a été défaillant dans l'emploi des moyens* (has failed in the use of best efforts).[42] This reflects the concept which underpins French law: the objective finding that the result is not achieved suffices to establish a failure in the case of a duty to achieve a specific result, whereas evidence of the obligor's fault must be shown in the case of a duty of best efforts.[43] Also, it must be observed that the defaulting obligor's

[38] Benedicte Favarque-Cosson and Denis Mazeaud, *European Contract Law. Materials for a Common Frame of Reference: Terminology, Guiding Principles, Model Rules,* (Munchen: Sellier, 2008), 208.

[39] At its 90th session the Governing Council of UNIDROIT (International Institute for the Unification of Private Law) adopted the third edition of the UNIDROIT Principles of International Commercial Contracts ("UNIDROIT Principles 2010").

[40] Comment of Article 5.1.4, UNIDROIT Principles 2010, p. 151, accessed on September 30, 2013, http://www.unidroit.org/english/principles/contracts/principles2010/integralversionprinciples2010-e.pdf.

[41] Id.; For instance, according to the comment of Article 5.1.4 in the UNIDROIT Principles 2010 report, this distinction signifies that more will be expected from a highly specialized firm selected for its expertise than from a less sophisticated partner.

[42] Christian von Bar and Ulrich Drobnig, *The interaction of contract law and tort and property law in Europe. A comparative study*, (Munchen: Sellier, 2004), 54.

[43] Favarque-Cosson and Mazeaud, *European Contract Law,* 209.

conduct is assessed in relation to an objective standard,[44] the good *pater familias* criterion.

The criterion which is most commonly acknowledged for the determination of the nature of an obligation is that of the "aleatory or otherwise character of the debtor's undertaking": if the promised performance can in the ordinary course of events be expected to be achieved, the obligation is *de resultat*; if not, it is an *obligation de moyens.*[45] Transposing this rule into the paradigm of the right to be forgotten, the nature of the obligation of the controller enshrined in Article 17(2) becomes obvious.

With regard to the correlative obligations of the right to be forgotten enshrined in Article 17, they are complex. On one hand, Article 17(1) entails a duty to achieve a specific result – the erasure of personal data on the given legal grounds, whereas Article 17(2) entails a duty of best efforts – to take all reasonable steps to inform third parties which are processing data that a data subject requests them to erase any links to, or copy or replication of that personal data. This is not an unusual situation, as Lando explained referring to contracts: "In some contracts part of a party's obligation is one of *resultat* and part of it one of *moyens*. A party, who has undertaken to deliver a computer with a programme which is aimed at performing certain functions, is strictly liable for the defects in the hardware but, unless he has warranted that the software can perform the desired functions, he is only obliged to make his best efforts to achieve that result".[46]

Therefore, the non-compliance of a controller with regard to the correlative obligations of the right to be forgotten will be established taking into account, on one hand the failure itself to erase data, pursuant to the duty to achieve a specific result in Article 17(1), and, on the other hand, the insufficient efforts to inform the third parties of the request to erase personal data made by the data subject, pursuant to the duty of best efforts in Article 17(2). This means that the controller will not be held liable under Article 17 of the DPR every time it fails to inform a third party of the erasure request.

With regard to the controller-processor differentiation,[47] even in the case of the existence of a processor, the responsible party for non-compliance with the duties enshrined in Article 17 remains the controller. For instance, in the French legal system, the principle which applies under Contract law is that the debtor of a duty is

[44] Id.

[45] Axel-Volmar Jaeger and Gotz-Sebastian Hok, *FIDIC – A Guide for Practitioners.* (Heidelberg, Dordrecht, London, New York: Springer, 2010), 21. The authors underline that, for instance, the obligation of an architect or engineer is sometimes said to be obligation *de moyens*, but in any case its obligations are *de resultat* in so far as the French decennial liability is concerned.

[46] Ole Lando, "Non-Performance (Breach) of Contracts", in *Towards a European Civil Code* 3rd ed., eds. Arthur S. Hartkamp et. al. (New York: Kluwer Law International, 2004), 504.

[47] The DPR proposal maintains the differentiation between "controller" and "processor" existing under Directive 95/46, defining the "processor" in Article 4(6) as "a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller".

also liable for non-fulfillment of his obligations if the non-fulfillment is caused by a person the debtor has employed to fulfill his obligations.[48] Such a principle can be used as an interpretative tool in the hypothesis of the liability of the controller whenever the data protection law does not provide otherwise. In the situation of the duty of best efforts, the data subject must prove that the "executant (processor) has made an error"[49] conducting the duty to inform third parties in order to engage the accountability of the controller.

The WP IEDP rephrased in its revision of the draft DPR the content of Article 17(2), maintaining nevertheless the character of a duty of best efforts: "Where the controller has made the personal data public and is obliged pursuant to paragraph 1 to erase the data, the controller, taking account of available technology and the cost of implementation, shall take reasonable steps, including technical measures, to inform controllers which are processing the data, that a data subject requests them to erase any links to, or copy or replication of that personal data". The question of the authorization is no longer at issue, the publication of the data being sufficient for the controller to know that it has to inform the subsequent controllers of that data. In addition, some criteria are added to assess whether the efforts of the controller were reasonable – "available technology" and "cost of implementation".

Article 17 of the draft DPR suffered modifications also in the LIBE compromise text. Article 17(1) provides that the data subject also "has the right to obtain from third parties the erasure of any links to, or copy or replication of the data". This obligation seems to be one of *resultat*, but it pertains to the third parties directly, and not to the data controller.

Article 17(2), in the LIBE text amending the DPR proposal, states that where the controller "made the personal data public without a justification based on Article 6(1), it shall take all reasonable steps to have the data erased, including by third parties, without prejudice to Article 77". There are three obvious differences compared to the correspondent text proposed by the EC. First, controllers are subject to this obligation only if they unlawfully made the personal data public – and not in all the cases. Second, the obligation envisages not only the information of third parties about the erasure request, but the erasure itself of data processed by third parties. And third, it specifies that the data subject shall further have the right to ask for damages in Court, even if the data will be erased by the controller and the third parties.

The norm still has the form of a duty of best efforts – "shall take all reasonable steps", but now it seems that even the obligation of the controller to erase personal data is an obligation of means whenever the data were made public – "to have the data erased, including by third parties". In the form adopted by LIBE, the matrix of correlative obligations for the right to erasure becomes even more complex, being enriched with an obligation of *resultat* for third parties and another obligation of *moyens* for the data controller.

[48] von Bar and Drobnig, *The interaction,* 148.

[49] Ibid.

Last, it must be underlined that not only the civil law systems distinguish between duties to achieve a result and duties of best efforts. In parallel, some common law provisions mirror the French distinction between these obligations, setting down for instance that a person who provides a service within his professional activity implicitly undertakes to provide the said service "with reasonable care and skill".[50,51] This is an instance of a duty of best efforts a violation of which will have to be proven and which may be contested by proving the absence of fault.[52]

9.4 The Characteristics of the Right to Erasure in the First Data Protection Laws in Europe

Some instances of the right to erasure of personal data were already enshrined in the different European laws with regard to the protection of personal data enacted before the adoption of the 1995 DPD.

According to the German data protection act (*Bundesdatenschutzgesetz*), enforced in 1977,[53] in principle "every data subject has the right to: [...] (4) erasure of stored data concerning him where such storage was inadmissible or – as an option to the right of blocking of data – where the original requirements for storage no longer apply".[54] Thus, the act also provided for an intermediary state between data used for processing and deleted data: "blocked data". Personal data that have been blocked may not be further processed or otherwise used, with a few exceptions.[55] Regarding the right to erasure, it presupposed that personal data may be erased when the information is no longer required for the purpose for which they were recorded and there is no reason to believe that the interests of the data subject would be thereby jeopardized. Personal data must be erased when storage is not permissible or where the data subject wishes to have them erased rather than blocked.[56]

[50] The UK Supply of Goods and Services Act 1982, Section 13.

[51] Favarque-Cosson and Mazeaud, *European Contract Law*, 217.

[52] Id.

[53] For the history of its enforcement, see Adriana C.M. Nugter, *Transborder Flow of Personal Data within EC*, (Amsterdam: Springer, 1990), 43.

[54] Section 4, *Bundesdatenschutzgesetz 1977.*

[55] Except for scientific purposes; to ameliorate evidentiary difficulties; if it is convincingly necessary in the interest of the data user or a third party; the data subject has given permission. (Section 27(2), corroborated with Section 14(2) third sentence, *Bundesdatenschutzgesetz 1977*).

[56] Section 26 *Bundesdatenschutzgesetz 1977.* See also Nugter (1990) at 62.

To this date, the German data protection law maintains the clear differentiation between erasure and blocking of data,[57] even though the DPD is evasive in this regard.

The French data protection law,[58] enforced in 1978, did not contain an explicit right to erasure. However, it provided for a "right to correction", which also entailed the "destruction" of data. The right to correction was laid down in Article 36 of the act, stating that if personal data are inaccurate, incomplete, ambiguous or out of date, or if the collection, use, disclosure to third parties or storage are prohibited, the data subject may have the data amended, supplemented, clarified, brought up-to-date or destroyed. Moreover, according to Article 38 of the French law, *the data user must inform third parties to whom the personal data were supplied that the data has since been corrected or destroyed.*[59] This provision resembles the obligation enshrined in Article 17 of the draft DPR.

UK's Data Protection Act from 1984 enshrined a right to rectification and erasure in Article 24, which provided that the data subject can submit an application to the court to request the rectification or erasure of inaccurate data and of any data held by the data user (the data controller) and containing an expression of opinion which appears to the court to be based on the inaccurate data. Hence, the erasure of data was granted to the data subject only if a court would find such a request justified.

Finally, the Dutch data protection act from 1989[60] also enshrined a right to erasure in Section 33(1), according to which every data subject has the right to request the data user in writing to correct, supplement or erase data if access has revealed that they are factually inaccurate, are incomplete for the purposes for which they were stored or are not relevant or appear in the file in contravention of a legal provision. The act further provided in Section 35 that unless the data subject waives this requirement, *the data user is obliged to communicate the correction, supplement or erasure to any third parties to whom he has knowingly disclosed the data concerned within a period of a year preceding the request for correction and up to the moment of the correction*. Moreover, the data subject shall be provided with a list of third parties who have been so informed.[61]

As a preliminary conclusion, the importance of erasing data from databases was recognized by the first legislators who created data protection laws. A pattern emerges from the erasure clauses: the data to be erased must always be inaccurate, the data usually have to be unnecessary for the purpose of their collection or the data must have been collected unlawfully. Some of the first legislators regulating data protection also envisaged an obligation for the processors of data to inform third parties to whom data were disclosed about the erasure or the rectification

[57] Section 20(3) of the German Federal Data Protection Act, as amended in 2009 by Article 1 of the Act of 14 August 2009.

[58] *Loi relative a l'informatique, aux fichiers et aux libertés*, which entered into force in 1978.

[59] Article 38, *Loi relative a l'informatique, aux fichiers et aux libertés 1978.*

[60] *Wet Persoonsregistraties,* enforced in 1989.

[61] For a characterization of the *Wet Persoonsregistraties* see Nugter, *Transborder Flow,* 145 et. seq.

of inaccurate/unnecessary[62]/unlawful data. Another common characteristic of the erasure clauses is that regulators did not substantially differentiate the conditions for erasure from those of rectification or blocking.

At the beginning of the nineteenth century, Benjamin Constant wrote about anonymity – *obscurité*, with an insight into the constitutive importance of the citizen's struggle for identity formation in a modern society.[63] A right to erasure of (inaccurate and unnecessary) personal data gathered in databases might have been the evident tool which would allow individuals to regain anonymity within the new computerized society.

9.5 The Right to Erasure and Its Correlative Obligations, in the Data Protection Directive

9.5.1 An Already Existing Right to Be Forgotten?

The scope of the Data Protection Directive of 1995 was the harmonization of data protection laws throughout the EU, which would protect the fundamental rights of the data subject, and also contribute to the free flow of data between Member States.[64] The choice of the European legislator to regulate the right to erasure under Article 12, which is entitled "the right to access", is rather curious. It can be explained by the fact that the right to erasure would be exercised only after the data subject would learn, pursuant to accessing her data, that the data are inaccurate.

The access right paves the way for a review of the processing, made directly by the data subject,[65] as the DPD completes the "right to know" with a series of

[62] By "unnecessary data", I mean data which are no more needed for the purposes of their initial processing.

[63] See de Hert, "The Case of Anonymity in western political philosophy. Benjamin Constant's refutation of republican and utilitarian arguments against anonymity" in *Digital Anonymity and the Law. Tensions and Dimensions,* eds. C. Nicoll, J.E.J Prins, M.J.M. van Dellen, (The Hague: T.M.C. Asser Press, 2003) at 49.

[64] It was only after the enactment of The Charter of Fundamental Rights of the European Union, which enshrines the right to the protection of personal data in Article 8, that the purpose of the EU data protection law became clear in that it is more connected with the protection of fundamental rights than with building the European market; See Paul de Hert and Serge Gutwirth, "Data Protection in the Case Law of Strasbourg and Luxemburg: Constitutionalism in Action", in *Reinventing Data Protection?*, eds. Serge Gutwirth, Yves Poullet et al., (Heidelberg: Springer, 2009), 9.

[65] For the interventional rights of the data subject, especially with regard to erasure of data, in a general context and also in specific processing contexts, see Lee A. Bygrave, *Data Protection Law – Approaching Its Rationale, Logic and Limits*, (New York, London, The Hague: Kluwer Law International, 2002), 65–66; Bart van der Sloot and Frederik Zuiderveen Borgesius "Google and Personal Data Protection", in *Google and the Law: Empirical Approaches to Legal Aspects of Knowledge-Economy Business Models,* ed. Aurelio Lopez Tarruella, (The Hague: Springer, 2012),

additional rights which were deemed in the literature to be designed to eliminate distorting factors and to restore the accuracy of the processing.[66] The DPD does not further prescribe what "blocking of data" means, nor does it explain when is a data subject entitled to ask for the blocking or erasure of data instead of rectification of data. Korff grammatically interpreted this incertitude through the use in English of the words "as appropriate" rather than "if [or when] appropriate", which suggests that controllers must take the measure "appropriate to" the particular demand. Therefore, if a data subject points out an inaccuracy, the appropriate measure is correction, and if the data subject establishes that data were excessive or irrelevant or unfairly or unlawfully obtained, the appropriate measure would be erasure – without the controller, or authorities or courts, if they were asked, having any discretion in the matter.[67] It is left entirely to the national courts of the Member States and the national data protection authorities to apply the transposing provisions of the right to erasure in accordance with the provisions of the Directive.[68]

With regard to the quality of the data to be rectified, erased or blocked, Article 12(b) is not limited to inaccurate or unnecessary data, but provides a fertile ground to protect the interests of the data subject whenever her data are processed unlawfully or unfairly.[69] More precisely, the DPD recognizes a general right to erasure of processed data when the controller or processor did not ground the processing in any of the six legal grounds provided in Article 7 DPD. An alternative condition which triggers the effectiveness of the right to erasure is the non-compliance with the five data quality principles in Article 6 DPD. For instance, a data subject could successfully argue that her data must be erased when they were collected and stored without a specified purpose, pursuant to Article 12(b) corroborated with Article 6(b) DPD.

The rectification, erasure and blocking of data are complemented by the controller's duty to notify third parties, to whom the data have been transmitted, of the necessary corrections,[70] according to Article 12(c) DPD. This duty is limited by a

103; Eleni Kosta and Diana M. Bowman, "Implanting implications: Data protection challenges arising from the use of human ICT implants", in *Human ICT Implants: Technical, Legal and Ethical Considerations*, eds. Mark N. Gasson, Diana M. Bowman, and Eleni Kosta, (The Hague: Springer, 2012), 106.

[66] Spiros Simitis, *Collected courses of the Academy of European Law*, Vol. VIII – 1, (The Hague: Kluwer Law International, 1997) at 132.

[67] Douwe Korff, *Data Protection Laws in the European Union*, (Federation of European Direct Marketing & Direct Marketing Association, 2005), 97.

[68] The duty of consistent interpretation with the provisions of a directive was established by the Court of Justice of the European Union in its decision from September 10, 1984 in Case C-14/83 *Von Colson and Kamann*, Rep. p. 1891. See also Sacha Prechal, *Directives in EC Law*, (Oxford: Oxford University Press, 2005), 180–216.

[69] The data subject can ask for the "… erasure or blocking of data *the processing of which does not comply with the provisions of this Directive*, in particular because of the incomplete or inaccurate nature of the data".

[70] Simitis, *Collected courses,* 132.

proportionality measure, as the controller is exempted to the notification of third parties when it is "impossible or involves a disproportionate effort". This restriction has been interpreted in the literature as not applying to "in house" situations, as "it cannot reasonably be said that to ever be impossible or disproportionate".[71] In the online context, such a duty could easily be deemed disproportionate or impossible. However, there is the question whether the controller could entirely disregard the notification duty or it is still obliged to at least make the effort to notify the third parties which could have had access to the rectified, erased or blocked information.

Another provision of the DPD which is of interest for the erasure of processed data is the general right to objection, enshrined in Article 14, which was deemed as being "an evident recognition of the right to self-determination".[72] According to it, the data subject has the right, "at least" when her data are processed based on the necessity for the performance of a task carried out in the public interest[73] or on the necessity for the purposes of the legitimate interests pursued by the controller,[74] to "object at any time on compelling legitimate grounds relating to his particular situation to the processing of data relating to him, save where otherwise provided by national legislation". This provision has been characterized as limited in scope,[75] as the Member States are not bound to introduce a right to objection in cases where the data subject has given her unambiguous consent, where the processing is necessary to perform a contract, a legal obligation or to protect a vital interest of the data subject.[76] Still, the Directive leaves it to the Member States to decide in which situation such a right should operate by clearly establishing a minimum standard with regard to Article 7 (e) and (f).

In addition, there is an absolute right to object enshrined in the DPD, from which states cannot legally derogate when transposing the directive, and it operates in the case of direct marketing (Article 14(b) DPD).

Simitis believes that the outcome of a successful objection would be to "block the use" of data.[77] In the paradigm of a right to be forgotten, this would mean that third parties, as well as the data subject, would not have access to certain information, which nevertheless continues to be stored by the controller, but not processed in any other way.

[71] Korff, *Data Protection Laws,* 98.

[72] Eleni Kosta, Aleksandra Kuczerawy, Ronald Leenes and Jos Dumortier, "Regulating Identity Management", in *Digital Privacy. PRIME – Privacy and Identity Management for Europe*, eds. Jan Camenisch, Ronald Leenes, Dieter Sommer, (Berlin, Heidelberg: Springer, 2011), 84.

[73] Article 7(e) DPD.

[74] Article 7(f) DPD

[75] Jef Ausloos, "The Right to be Forgotten – Worth Remembering?", *Computers Law and Security Review 28* (2012): 150.

[76] Article 7 (a), (b), (c), (d) DPD.

[77] Simitis, *Collected Courses,* 130.

9.5.2 The Application in Practice of the Erasure and Objection Clauses: Google v. Spain, a Cornerstone Case

The Court of Justice of the European Union (CJEU) did not have the opportunity until now to clarify the content of these provisions through the preliminary ruling procedure, which allows national courts of the Member States to ask the CJEU to clarify certain provisions of EU law in order to correctly apply them in a specific case before them.[78] A particular case brought by Audiencia Nacional, a Spanish court, to the CJEU, in March 2012, is of utmost importance for the right to be forgotten debate, especially because it is brought against a search engine (Google).[79] The case concerns a Spanish citizen who wants an article containing his personal data, published in the Spanish newspaper "La Vanguardia Ediciones", to be erased, or, if that is not possible, he wants the article not to appear in the search results when his name is searched through Google. He claims that the piece of information concerns an old debt, which has long been paid off. His both requests were rejected by the newspaper and Google Spain, which took the view that the request should be sent to the headquarters of Google in the United States. He further complained to the Spanish Data Protection Authority (DPA), which declined the request to order the newspaper to delete the article, but released an order addressed to Google Spain "to take the necessary steps to retrieve the concerned data from its search index and to make the future access impossible to these data".[80] Google contested the decision in court.

Audiencia Nacional took the view that this dispute "envisages the protection of personal data, and more precisely the rights to erasure, blocking and objection of the data subject exercised against the activity of the providers of engines which search information on the internet".[81] It decided that all of the legal issues involved in the case at hand need further clarification from the CJEU, starting with establishing jurisdiction and ending with the clarifying question of the liability of Google under the erasure and objection clauses from the current DPD. It asked whether the national DPA "protecting the rights embodied in Articles 12(b) and 14(a) of Directive 95/46/EC could directly impose on the search engine of the Google undertaking a requirement that it withdraw from its indexes an item of information published by third parties, without addressing itself in advance or simultaneously to the owner of the web page on which that information is located".[82]

[78] Article 267 of the Treaty on the Functioning of the European Union.

[79] Case C-131/12, Reference for a preliminary ruling from the Audiencia Nacional (Spain) lodged on 9 March 2012 – Google Spain, S.L., Google Inc. v Agencia Española de Protección de Datos, Mario Costeja González, pending.

[80] Audiencia Nacional, Recurso 725/2010, Sala de lo Contencioso-Administrativo. Sección 1ª, from February 2, 2012 (translation of the author).

[81] Id. (t.a.).

[82] Case C-131/12 (n 79), question 2.3.

Even though the current framework was deemed "inadequate" in previous literature,[83] this case indicates that the provisions of Directive 95/46 are likely to be interpreted in the sense of an already existing right to be forgotten, which has a piecemeal structure and which needs a dynamic interpretation to become effective. Such an interpretation has already been given by the Spanish DPA, and convinced a high court of a Member State to raise detailed and clear questions to the CJEU in the matter of search engines as enablers of forgetting information.

In spite of the fact that some existing provisions of the European data protection legal framework can be interpreted as an already existing right to be forgotten provisions, the truth remains that, currently, the EU legal framework does not provide for a general and explicit right to be forgotten.[84]

In fact, Advocate General Jääskinen affirmed in his Opinion in the Google vs. Spain case that the Data Protection Directive "does not provide for a general right to be forgotten in the sense that a data subject is entitled to restrict or terminate dissemination of personal data that he considers to be harmful or contrary to his interests".[85] He also added that the criteria to be applied for deciding upon a deletion request, when data is processed without the subject's consent, are (1) the purpose of processing and (2) the interests served by it.[86] After providing for this two stages test, AG Jääskinen did not further apply it. He merely underlined that "a subjective preference alone does not amount to a compelling legitimate ground within the meaning of Article 14(a) of the Directive".[87]

9.6 Conclusion

Benjamin Constant defended obscurity almost two centuries before the computer age and the information society. As it was summarized by de Hert, "[h]is argument is straightforward: denying anonymity is to deny liberty. Recognition of anonymity is not only desirable for the protection of ideas, but for all aspects of individual liberty. It hampers individual self-realization and lowers the ethical quality of a given society. A fear of identification, monitoring, and surveillance may well increase citizens' general distrust of politics and government institutions".[88]

[83] Ausloos *The Right to Be Forgotten,* 145. The critique is mainly based on the weakness of consent rules in the DPD, even though the more technical rights to erasure and object are more akin to a right to be forgotten than withdrawal of consent for the ongoing processing, which only produces effects for the future.

[84] Ambrose and Ausloos, *The Right to Be Forgotten,* 7.

[85] Opinion of Advocate General Jääskinen delivered on 25 June 2013 in Case C-131/12 *Google Spain* vs. *Agencia Espanola de Proteccion de Datos*, para. 108.

[86] Id.

[87] Id.

[88] de Hert, *The case of Anonimity,* 49.

Even if technically speaking the right to be forgotten is an upgraded right to erasure, it represents more: it stands for the autonomy, liberty, and identity of the person in an over-digitalized world. These fundamental values are inherent to the human being and it will be more and more difficult to define geographically the instruments which will preserve such values.

The right to be forgotten as "the biggest threat to free speech on the Internet in the coming decade"[89] proves to be more of a myth. In fact, the right to erasure of personal data, sometimes followed by the duty to inform third parties of the erasure request, was enshrined in the European data protection laws since the '70s, and it is also provided for in the Data Protection Directive. The provision proposed in Article 17 of the draft DPR does not create a new right, but it clarifies and strengthens the right to erasure. It does not even mention any of the derivates of the verbs "to forget" or "to be forgotten".

The most controversial provision – the obligation to inform third parties, is merely a duty of best efforts, the controller not being obliged by law to obtain the erasure of the data in question from every single third party that processed it, but only to use its best efforts to inform the third parties about the erasure request.

A significant part of the right to be forgotten myth is the fear that it will affect in an unprecedented way freedom of expression. In fact, the exception first enumerated in the DPR proposal under Article 17 is freedom of expression. European national and supranational courts have a rich history in balancing freedom of expression and other opposing fundamental rights in order to find an accepted equilibrium. There are no reasons to believe that the European Courts will disrupt the tradition of finding equilibrium between opposing rights when faced with the tension between the right to be forgotten and freedom of expression.

Another remark should be made regarding the current variations of the DPR proposal text of Article 17, emerged during the legislative process. This paper analyzed a working document of the Council and the final position of the LIBE Committee, which will be used as starting point in the future negotiations on the regulation. Studying both variations of the norm, one conclusion is that the underlying idea of the right to be forgotten – erasure of personal data by controllers and third parties, is not going away. In a form or another, it will be regulated in a complex manner in the future regulation and it is statistically more likely that the view of the Council will be the more prominent one in the final form of the DPR.[90]

[89] Rosen, *The right to be forgotten.*

[90] According to a study which employed an automated text comparison technique (Wordfish), "the joint texts produced by the (conciliation) committee are more similar to the prior positions of the Council, than that of the Parliament"; "69,3 % close to the Council; 30,1 % close to the Parliament; 0,6 % close to both"; Camilla Mariotto and Fabio Franchino, *Explaining Outcomes of Conciliation Committee's Negotiations*, presented at the "Decision-making before and after Lisbon" Workshop (DEUBAL), on November 3–4 2011, University of Leiden. Available on http://www.ces.ufl.edu/documents/pdf/deubal/workshops/2011/FranchinoMariotto_DEUBAL_110411.pdf, last accessed on 11 January 2014.

The development of the online world makes the effectiveness of the right to be forgotten challenging. While it is true that "temporal oriented solutions to cope with the impression management-undermining characteristics of the Internet like the 'right to be forgotten or erasure' in the General Data Protection Regulation will not be of any help for 'actors' who want to be able to play different roles in the same timeframe",[91] it is also true that the lifestream[92] of the Internet developed in recent years justifies also a temporal dimension of the solutions stemming from the right to be forgotten.

Acknowledgements I would like to thank the CPDP reviewers for their comments and suggestions for the improvement of this paper.

Disclaimer The opinions expressed in the paper pertain exclusively to the author and do not engage in any way the EDPS.

References

Ambrose, Meg Leta and Ausloos, Jef. 2012. "The right to be forgotten across the pond", Telecommunications Policy Research Conference, available on http://ssrn.com/abstract=2032325, last accessed on 11 January 2014.

Ausloos, Jef. 2012. *The Right to be Forgotten – Worth Remembering?*, Computers Law and Security Review 28: 143–152.

Bejan, Adrian and Lorente, Sylvie. 2010. "The constructal law of design and evolution in nature", *Philosophical Transactions of the Royal Society of London* 365: 1335–1347. doi: 10.1098/rstb.2009.0302.

Bernal, Paul. 2014. "The EU, the US and Right to be Forgotten", in *Reloading Data Protection. Multidisciplinary Insights and Contemporary Challenges,* eds. S. Gutwirth, R. Leenes, P. de Hert eds., 61–77. Dordrecht, Heidelberg, London, New York: Springer.

Brüggemeier, Gert, Colombi Ciacchi, Aurelia and O'Callaghan, Peter. 2010. *Personality Rights in European Tort Law*, New York: Cambridge University Press.

Bygrave, Lee A.. 2002. *Data Protection Law – Approaching Its Rationale, Logic and Limits*. New York, London, The Hague: Kluwer Law International.

de Hert, Paul and Gutwirth, Serge. 2009. *Data Protection in the Case Law of Strasbourg and Luxemburg: Constitutionalism in Action*, in Serge Gutwirth, Yves Poullet et al. (eds.), *Reinventing Data Protection?*, 3–44. Heidelberg: Springer.

de Hert, Paul. 2003. "The Case of Anonymity in western political philosophy. Benjamin Constant's refutation of republican and utilitarian arguments against anonymity" in eds. C. Nicoll, J.E.J. Prins, M.J.M. van Dellen, *Digital Anonymity and the Law. Tensions and Dimensions,* 47–98. The Hague: T.M.C. Asser Press.

[91] Paulan Korenhof, "Seconds of Distance. An analysis of the audience segregation in space and time with regard to different online impression management issues", *TILT Law and Technology Working Paper* 1 (2013): 10.

[92] As Gelernter (2013) explains, "this lifestream — a heterogeneous, content-searchable, real-time messaging stream — arrived in the form of blog posts and RSS feeds, Twitter and other chatstreams, and Facebook walls and timelines. Its structure represented a shift beyond the 'flatland known as the desktop' (where our interfaces ignored the temporal dimension) towards streams, which flow and can therefore serve as a concrete representation of time".

Farivar, Cyrus. 2013. "Proposed EU data protection reform could start a trade war, US official says", ArsTechnica, 1 February, http://arstechnica.com/tech-policy/2013/01/proposed-eu-data-protection-reform-could-start-a-trade-war-us-official-says/, accessed on 11 January 2014.

Favarque-Cosson, Benedicte and Mazeaud, Denis. 2008. *European Contract Law. Materials for a Common Frame of Reference: Terminology, Guiding Principles, Model Rules.* Munchen: Sellier.

Gelernter, David. 2013. "The End of the Web, Search, and Computer as We Know It", *Wired*, 1 February. http://www.wired.com/opinion/2013/02/the-end-of-the-web-computers-and-search-as-we-know-it/ : accessed January 11, 2014.

Henkin, Louis. 1974. "Privacy and Autonomy", *Columbia Law Review* 74, vol. 8: 1410–1433.

Hilbert, Martin and Lopez, Priscila. 2011. "The World's Technological Capacity to Store, Communicate, and Compute Information", *Science* 332: 60–65.

Hondius, Frits W.. 1975. *Emerging Data Protection in Europe*. Amsterdam: North-Holland Publishing Company; New York: American Elsevier Publishing Company.

Jaeger, Axel-Volkmar and Hok, Gotz-Sebastian. 2010. *FIDIC – A Guide for Practitioners.* Heidelberg, Dordrecht, London, New York: Springer.

Koops, Bert-Jaap. 2012. 'Forgetting Footprints, Shunning Shadows. A Critical Analysis of the "Right to be Forgotten" in Big Data Practice', *Tilburg Law School Legal Studies Research Paper Series* 8.

Korenhof, Paulan. "Seconds of Distance. An analysis of the audience segregation in space and time with regard to different online impression management issues", *TILT Law and Technology Working Paper* 1 (2013), 10.

Korff, Douwe. 2005. *Data Protection Laws in the European Union*. Federation of European Direct Marketing & Direct Marketing Association.

Kosta, Eleni and Bowman, Diana M.. 2012. "Implanting implications: Data protection challenges arising from the use of human ICT implants", in eds. Mark N. Gasson, Diana M. Bowman, and Eleni Kosta, *Human ICT Implants: Technical, Legal and Ethical Considerations*, 97–113. The Hague: Springer.

Kosta, Eleni, Kuczerawy, Aleksandra, Leenes, Ronald and Dumortier, Jos. 2011. Regulating Identity Management, in eds. Jan Camenisch, Ronald Leenes, Dieter Sommer, *Digital Privacy. PRIME – Privacy and Identity Management for Europe*, 73–90. Berlin, Heidelberg: Springer.

Lando, Ole. 2004. "Non-Performance (Breach) of Contracts", in eds. Arthur S. Hartkamp et. al., *Towards a European Civil Code* 3rd ed, 504–515. New York: Kluwer Law International.

Mariotto, Camilla and Franchino, Fabio. 2011. *Explaining Outcomes of Conciliation Committee's Negotiations*, presented at the "Decision-making before and after Lisbon" Workshop (DEUBAL), on November 3–4 2011, University of Leiden. Available on http://www.ces.ufl.edu/documents/pdf/deubal/workshops/2011/FranchinoMariotto_DEUBAL_110411.pdf, last accessed on 11 January 2014.

Mayer-Schönberger, Viktor. 2009. *delete. The Virtue of Forgetting in the Digital Age.* Princeton University Press.

McNealy, Jasmine E..2012. "The emerging conflict between newsworthiness and the right to be forgotten", *Northern Kentucky Law Review*, vol. 39:2: 119–135.

Nugter, Adriana C.M.. 1990. *Transborder Flow of Personal Data within EC*. Amsterdam: Springer.

Prechal, Sacha. 2005. *Directives in EC Law*. Oxford: Oxford University Press.

Rosen, Jeffrey. 2012. "The Right to be Forgotten" 64 Stanford Law Review Online 88.

Rouvroy, Antoinette and Poullet, Yves. 2009. "The Right to Informational Self-Determination and the Value of Self-Development: Reassessing the Importance of Privacy for Democracy," in *Reinventing Data Protection?*, ed. Serge Gutwirth et. al., 45–75. Springer Science + Business Media B.V.

Simitis, Spiros. 1997. *Collected courses of the Academy of European Law*, Vol. VIII – 1. The Hague: Kluwer Law International.

Tene, Omer and Wolf, Christopher. 2013. *Overextended: Jurisdiction and Applicable Law under the EU General Data Protection Regulation* White Paper. Available on http://www.futureofprivacy.org/wp-content/uploads/FINAL-Future-of-Privacy-Forum-White-Paper-on-Jurisdiction-and-Applicable-Law-January-20134.pdf, last accessed on 11 January 2014.

Tene, Omer and Polonetsky, Jules. 2013. ‘Judged by the Tin Man: Individual Rights in the Age of Big Data’, *Journal of Telecommunications and High Technology Law*, forthcoming, available at SSRN http://ssrn.com/abstract=2311040, last accessed on 11 January 2014.

van der Sloot, Bart and Zuiderveen Borgesius, Frederik. 2012. *Google and Personal Data Protection*, in ed. Aurelio Lopez Tarruella, *Google and the Law: Empirical Approaches to Legal Aspects of Knowledge-Economy Business Models,* 75–111. The Hague: Springer.

von Bar, Christian and Drobnig, Ulrich. 2004. *The interaction of contract law and tort and property law in Europe. A comparative study*. Munchen: Sellier.

Walker, Robert Kirk. 2012. “The Right to be Forgotten”, *Hastings Law Journal* 64: 101–129.

Wardwell, James and Smith, G. Stevenson. 2008. “Recovering erased digital evidence from CD-RW disk in a child exploitation investigation”, *Digital Investigation* Vol. 5, 1–2: 6–9.

Westin, Alan F. 1967. *Privacy and Freedom*. New York: Atheneum.

Whitman, James Q..2004. “The Two Western Cultures of Privacy: Dignity Versus Liberty”, *Yale Law Journal*, 113: 1151 – 1194.

Zanfir, Gabriela. 2014. “Forgetting about consent. Why the focus should be on suitable safeguards in data protection law” in *Reloading Data Protection. Multidisciplinary Insights and Contemporary Challenges,* eds. S. Gutwirth, R. Leenes, P. de Hert eds., 237–257. Dordrecht, Heidelberg, London, New York: Springer.

Part IV
Does It Take Two to Tango: Privacy and Security?

Chapter 10
Privacy Versus Security: Problems and Possibilities for the Trade-Off Model

Govert Valkenburg

Abstract Considerable criticism has been levelled against thinking of privacy and security as being placed in a trade-off relation. Accepting this criticism, this paper explores to what use the trade-off model can still be put thereafter. In specific situations, it makes sense to think of privacy and security as simple concepts that are related in the form of a trade-off, even though it has been argued widely that this is a misrepresentation of concepts that are far too complex to be thought of in such a simple structure. As a first step, the sociotechnical analysis in this paper further highlights the complexities of the practice of body scanners installed at airports for security purposes. These complexities contribute additionally to rendering a simple privacy/security trade-off untenable. However, as a second step, the same analysis is thought through again so as to highlight opportunities to use the – deliberately simple – structure of the trade-off model to overcome part of its own shortcomings. At closer look, the empirical inaccuracy of the trade-off model becomes only problematic if it is used as a justification for imposing security measures that encroach privacy: "this small piece of privacy must be sacrificed, as this additional security is indispensable". However, some right to existence is still retained for the trade-off model. Therefore, instead, it is suggested that the trade-off model be used on the one hand as a heuristic device to trace potential difficulties in the application of a security technology, and on the other hand as a framing that by its simplicity and appeal earns impetus for a particular discourse.

Keywords Privacy • Security • Tradeoff • Airport security

10.1 The Trade-Off Model Between Privacy and Security

Privacy and security are oftentimes discussed as if they are simply opposing concepts; as if a trade-off exists between them. This trade-off between privacy and security has long been criticized as untenable, chiefly because the complexity and multiplicity of either value are incompatible with such a simple relation. At the

G. Valkenburg (✉)
Faculty of Arts and Social Sciences, Maastricht University, Maastricht, The Netherlands
e-mail: g.valkenburg@maastrichtuniversity.nl

S. Gutwirth et al. (eds.), *Reforming European Data Protection Law*,
Law, Governance and Technology Series 20, DOI 10.1007/978-94-017-9385-8_10

same time, the trade-off vocabulary of is remarkably persistent in various discourses, notably in policy. This persistence suggests that there is something attractive in the model, even though it is from some perspectives plain incorrect. This paper explores one possible function the trade-off model might yet fulfil, despite its empirical inaccuracy: its use as a heuristic model to highlight particular interests in debates.

In its general form, the trade-off model thinks of privacy and security as two simple concepts, which relate in such a way that promoting one of them leads to deteriorating the other. The idea is attractive for its simplicity. President Obama used the motive literally in defence of (parts of) the NSA activities revealed by Edward Snowden.[1] Also European policy making is pervasively troubled by thinking in terms of a trade-off.[2] Apart from the simplicity ingrained in this and similar trade-offs, the rhetoric is also powerful in the particular case of privacy versus security: the latter easily trumps the former, and who would not give up some of their privacy if it helps preventing terrorist attacks?[3] This even works if the security risks are poorly specified,[4] and it certainly works against the background of an increasing pervasiveness of identifications of threats.[5]

A range of criticisms have been produced against the model, which can be roughly divided in two clusters. On the one hand, there are the internal criticisms that address the validity of the model. Their bottom line is that at the end of the day, the overly simplistic representation offered by the trade-off model can never accurately represent the complexities and intricacies of how privacy and security are implemented in practice. On the other hand, criticisms are offered that I call external, which concern how the model is used. In general, they hold that the model is typically used to impose fallacious choices on a public.[6]

Regarding the internal validity of the model, it is often argued that the concepts of privacy and security are not simple but instead complex. From their heterogeneous constituents, it is hard if not impossible to articulate how such a zero-sum relation would be produced.[7] The simplicity is already disproved by the fact that both

[1] Euronews, "Obama Defends 'Privacy Trade-Off' for Security," http://www.euronews.com/2013/06/07/obama-defends-privacy-trade-off-for-security/.

[2] Marc van Lieshout et al., "Reconciling Privacy and Security," *Innovation: The European Journal of Social Science Research* 26, no. 1–2 (2013).

[3] Daniel J. Solove, ""I've Got Nothing to Hide" and Other Misunderstandings of Privacy," (2007); *Nothing to Hide: The False Tradeoff between Privacy and Security* (New Haven, London: Yale University Press, 2011); Jennifer Chandler, "Privacy Versus National Security: Clarifying the Trade-Off," in *On the Identity Trail: Anonymity, Privacy and Identity in a Networked Society*, ed. Ian Kerr, Valerie Steeves, and Carole Lucock (Oxford: Oxford University Press, 2009).

[4] George Gaskell et al., "Gm Foods and the Misperception of Risk Perception," *Risk Analysis* 24, no. 1 (2004).

[5] Louise Amoore, "Biometric Borders: Governing Mobilities in the War on Terror," *Political Geography* 25, no. 3 (2006).

[6] Solove, *Nothing to Hide: The False Tradeoff between Privacy and Security*.

[7] David Wright et al., "Privacy, Trust and Policy-Making: Challenges and Responses," *Computer Law & Security Review* 25, no. 1 (2009).

security and privacy are radically differently enshrined in EU and US laws, respectively.[8] Similarly, the model is argued to neglect the many examples of interventions being good both for privacy and for security, and even interventions that promote security *through* the promotion of privacy or the other way round.[9] For example, it is conceivable that citizens are secured against abuse of state power by installing particular privacy-promoting sociotechnical configurations. The model also neglects examples where privacy or security is compromised without a clear benefit for the other side. Finally, even if the trade-off model in some particular situation appears valid, it will certainly merit some further qualification as to its limits.[10] Even then, a complete sacrifice of one in favour of the other is still very likely to be unacceptable.

Regarding the use of the model, a different kind of criticism has been voiced. Schneier[11] for example argues that the trade-off model is typically mobilized as a false choice for people: citizens are asked to give up some of their basic liberties in return for security. What makes things worse is that this security and risks are typically poorly specified and not self-evident.[12] Additionally, Chandler[13] argues that the model is intrinsically biased: when posed in opposition, security easily trumps privacy. After all, a lack of security is potentially life-threatening, whereas a lack of privacy is not. Also, it has been observed that public perceptions are more intricate and elaborate than a simple trade-off.[14] In similar vein, it has been observed that it is impossible to predict how any balance between privacy and security would be struck by the general public, if only because the public's trust in authorities importantly influences how such a balance would be struck.[15] The resulting policy is also rather diverse across states.[16] In a way, many uses to which the trade-off model is put, render public perception, public opinion making and policy making a bit of a caricature.

This paper develops a double perspective on the trade-off model, developing the empirical problematicity as well as the practical usability of the model. Importantly,

[8] Lauren B. Movius, "U.S. And Eu Privacy Policy: Comparison of Regulatory Approaches," *International Journal of Communication* 3(2009).

[9] Lee S. Strickland and Laura E. Hunt, "Technology, Security, and Individual Privacy: New Tools, New Threats, and New Public Perceptions," *Journal of the American Society for Information Science and Technology* 56, no. 3 (2005).

[10] Solove, *Nothing to Hide: The False Tradeoff between Privacy and Security*.

[11] Bruce Schneier, "Protecting Privacy and Liberty. The Events of 11 September Offer a Rare Chance to Rethink Public Security," *Nature* 413, no. 25 October 2001 (2001).

[12] Gaskell et al., "Gm Foods and the Misperception of Risk Perception."

[13] Chandler, "Privacy Versus National Security: Clarifying the Trade-Off."

[14] Vincenzo Pavone and Sara Degli Esposti, "Public Assessment of New Surveillance-Oriented Security Technologies: Beyond the Trade-Off between Privacy and Security," *Public Understanding of Science* 21, no. 5 (2012).

[15] Darren W. Davis and Brian D. Silver, "Civil Liberties Vs. Security: Public Opinion in the Context of the Terrorist Attacks on America," *American Journal of Political Science* (2004).

[16] Movius, "U.S. And Eu Privacy Policy: Comparison of Regulatory Approaches."

the analysis is not intended to provide a conclusive account of all that matters in privacy and security studies, but to highlight only one exemplary couple of values, namely privacy and security, and how they might be thought to relate to thinking in terms of a trade-off model. The generalization and extension of this ideal-typical way of thinking is then left to further scholarship.

First, the internal line of criticism levelled against the trade-off model is furthered by empirical analysis. A sociotechnical analysis is presented of *active-millimetre wave* body scanners used in airport security. This analysis adds yet another reason why the trade-off model is in some respects too simple. As will become clear, sociotechnical practices are not the clear-cut implementations of generic design values such as security and privacy. Rather, their development is full of contingencies, particularities, and connections to context in any conceivable sense. These connections render the versions of privacy and security that are eventually found on the work floor of airport security very much particular, contingent and heterogeneous. This analysis adds further complexities in face of which the trade-off model indeed appears as hopelessly oversimplified.

Second, rather than stopping at just another blow to the trade-off model, the paper derives from the same sociotechnical perspective arguments that support a particular use of the model. Indeed, the trade-off model would be problematically oversimplified if it were used as a *representational* model, a model that structures our understanding of reality. Indeed, if such an alleged misrepresentation is used discursively and in pursuit of particular justifications, the external critiques just mentioned cut ice. However, uses of models are much more diverse than only representational. Particularly in policy contexts, models rather serve to organize intervention. Even if they do not offer the most accurate empirical representation, they may still serve to explain and inform decisions and provide legitimacy to intervention. I refer to models used this way as *interventional* models. Taking warning from the aforementioned external critiques, the challenge is to find a way to use models in this interventional way, without incurring the critique of playing inconsiderate discursive games. It must be borne in mind that simplification is often key to arriving at an intervention in the first place. The trade-off model might offer just the simplification needed there, and that is what this paper will continue to investigate. (In the following, the trade-off model will be approached in a rather monolithic way without much further internal differentiation, which is legitimated by the level of analysis at which the broader argument of this paper is situated.)

This paper is organized as follows. In the second section, the sociotechnical practice of airport scanners will be dissected into some of the underlying configurations, so as to articulate how particular versions of privacy and security emerge in the end. In the third section, it will be explored how models can be made productive in policy context, especially against the background of the complexity articulated in the sociotechnical analysis. In the fourth section, the particular sociotechnical analysis of airports scanners will be connected back to the idea of interventional use of models, and explore how the trade-off model in particular can function as one such model.

10.2 Inside Airport Security Scanners

In order to seek fertile ground on which the trade-off model can flourish, technological developments in airport security offer an interesting research site. This paper focuses on one particular type of body scanner, which has over the past few years been introduced at airports. This particular type works by means of millimetre waves, by which it detects objects hidden under the clothes. Upon detection, the scanner informs the security officer by means of a generic mannequin. On this mannequin, only those body parts are highlighted on which a suspect object is found. (In due course, the intricacies will be discussed of how this mannequin representation is created, both in terms of its technical implementation and in terms of its privacy implications.)

This *active millimetre wave* variety of body scanners has been researched through five expert interviews with developers, policy makers and security operators. Additional background information was sought, mainly from academic and internet sources. The research intent has not been to provide a comprehensive account of body scanning technologies, but rather to provide an ideal-typical analysis of how privacy and security appear once a cross-section is made through development and application. This cross-section provides for articulation of connections between privacy and security, such that, again ideal-typically, legitimate and fruitful uses of the trade-off model can be identified.

At face value, the scanner setup described above has some important advantages. First, privacy seems to be respected because no actual picture of the body is made, nor is such a picture displayed. Second, manual body searches are expected to decrease in numbers and manual body searches will in general be less burdensome as they can be directed at specific body parts, not the whole body. Third, the automatic assessment is argued to make the whole airport security process quicker. This means that the process will be more efficient and less costly, but also offer a better customer experience for the traveller. It must be noted that the idea of privacy underlying the present analysis is not some fixed concept such as the famous original notion framed by Warren and Brandeis[17] or more recent dissections of the general idea.[18] Rather, focus is directed at what goes in practice under the heading of privacy; how privacy is 'performed'.

While this seems like a greatly privacy respecting implementation of security, implementation of security (or any other design goal in general, for that matter) is never the straightforward application of a universal idea of security. It is always a *particular* idea of security, geared towards a *particular* practice. Implementation of such a particular form of security into security technologies will always be an implementation against the backdrop of a particular technological state of the

[17] Samuel Warren and Louis D. Brandeis, "The Right to Privacy," *Harvard Law Review* 193(1890).

[18] Rachel L. Finn, David Wright, and Michael Friedewald, "Seven Types of Privacy," in *European Data Protection: Coming of Age*, ed. Serge Gutwirth and Yves Poullet (Dordrecht: Springer, 2013).

art – not just anything is possible – legal and regulatory frameworks – not just anything is allowed – and many other stakes and interests such as procedural efficiency, customer satisfaction, and all elements of the context upon which the design and operation of the security technology are contingent. Only if all these contingencies are taken into account, it can be made intelligible why and how particular versions of privacy and security become 'enacted' in practice.[19]

To begin at the end, through this particular sociotechnical configuration, security becomes enacted as the detection of materials other than skin and clothing. As one interviewee explains, the scanner is said to detect 'anomalies', or literally 'things that cannot be classified'. This seems legitimate, as skin and clothing are typically the things that we would happily allow on board airplanes. However, on second thought, it is not all that clear that this accurately defines the fault line between safe and dangerous items. While the set of anomalies or 'suspect items' is indeed likely to include most of the things we do not want inside airplanes, it is also very likely to include a lot of things that should not be particularly worrisome. Indeed, in practice, as another interviewee explains something as innocent as a business card in a chest pocket triggers an alarm. Thus, the body scanner does not straightforwardly outperform conventional walk-through metal detectors in a quantitative sense when comes to false alarms. Rather, it produces very *different* false alarms from a qualitative perspective (which may, ultimately, still make a quantitative difference).

Similarly, privacy is enacted in the end as the elimination of body details – recall that the mannequin does not resemble an actual body. However, below this apparent neutral and impersonal look, numerous normative choices hide. For the technology to be able to assess whether something is suspect about a passenger, it needs to be inscribed with extensive assumptions about what a 'normal' body is: what normal body shapes and sizes are and what a skin's normal reflection pattern is under illumination by millimetre waves. In the machine, these assumptions are translated primarily into assumptions of what a 'normal' millimetre-wave reflection pattern is. Typically, technologies perform such assumptions rather rigidly and indiscriminately. In this case, the technology renders abnormal those bodies that do not fit. As there is no such thing as a universal, normal body, it is likely that false alarms are triggered. Such false alarms *de facto* render some people abnormal.

Even though the scanner setup was intended to be privacy-respecting and to leave people's abnormalities undisclosed much like the ways people also conceal such abnormalities in other spheres of life, it actually makes those abnormalities more visible. True enough, it does not do so by putting a nude picture on a screen. Instead, it does so by raising a false alarm, drawing attention to a person, and effectively forcing the person into exposing and explaining their abnormality. This abnormality

[19] For 'enactment', see John Law, "Actor Network Theory and Material Semiotics," in *The New Blackwell Companion to Social Theory*, ed. Bryan S. Turner (Chichester: Blackwell, 2009); John Law and John Urry, "Enacting the Social," *Economy and Society* 33, no. 3 (2004); John Law, *After Method: Mess in Social Science Research* (London, New York: Routledge, 2004).

will in most cases have nothing to do with the bomb-belt terrorists who initially served as the justification for the scanner to be installed. Rather, it reflects what was assumed to be a normal body and a normal reflection pattern in the course of developing the device.

It has been reported by multiple interviewees that people carrying medical devices such as stomas and pace makers trigger alarms. With stoma patients, embarrassing situations have been reported: alarms were indeed raised and explanation was demanded on the spot. Even after moving to a secluded inspection room, some difficulties remained. Particularly, running water is not always available in such rooms, even though it is needed in case the medical devices become dislocated. To prevent discomfort, the Dutch stoma patients' association has agreed with security officials that stoma patients may identify themselves beforehand to security personnel, upon which they be treated in a more prudent way. Even though the 'problem' of stoma patients has been settled in a way that is accepted by both the stoma patients' association and the security operators, it is still a peculiar translation of privacy. Apparently, privacy *for stoma patients* consists ironically of announcing: 'I am a stoma patient'. All in all, part of the privacy challenge is not really solved, but 'displaced' to a particular burden put on colostomy patients.

This problem of bodies that are classified as abnormal is more endemic than only affecting the group of stoma patients: it has even been reported by one frequent flyer that he consistently triggers an alarm for which no reason could be identified on the spot – other than apparently some unspecified abnormality of the body. (Clearly some reasons such as sweat are principally known, but this is not to say that such explanations are practically available when an alarm is triggered, nor that they would suffice, to the complex background of airport security, to discard the alarm.) What appears first as a mere unfortunate technical difficulty of assessing particular bodies, is in fact the reflection of a strong normalization of the body that is inscribed in airport security technologies.

The negotiations that go into the configuration of the security scanner and its surrounding practice, can best be understood as a chain of *translations*.[20] In each step of implementation, a negotiation takes place in which stakes and interests are balanced, and goals accordingly redefined. These translations entail that in the seemingly simple, technological implementation of ideas such as privacy and security, in the end considerable redefinitions of those concepts become visible: rearrangements and redefinitions of political interests, technical options, and airport operations were needed such that this particular scanner came to be feasible.

[20] Bruno Latour, *Science in Action - How to Follow Scientists and Engineers through Society* (Cambridge MA: Harvard University Press, 1987); Michel Callon, "Some Elements of a Sociology of Translation: Domestication of the Scallops and the Fishermen of Saint Brieuc Bay," in *Power, Action and Belief: A New Sociology of Knowledge?*, ed. John Law (London: Routledge and Kegan Paul, 1986); Madeleine Akrich and Bruno Latour, "A Summary of a Convenient Vocabulary for the Semiotics of Human and Nonhuman Assemblies," in *Shaping Technology, Building Society: Studies in Sociotechnical Change*, ed. W. E. Bijker and J. Law (Cambridge, MA: MIT Press, 1992).

No single choice is arbitrary, and each choice bears on the enactments that emerge in the end. For instance, the mm-wave spectrum was selected because of its commonly accepted harmlessness. Also, the waves are agreed upon not to enter the body. However, the wavelength also entails that a poorer level of detail is achieved than would be the case with imaging technologies based on visible or infrared light, or with X-rays (where it should be noted that imaging technologies based on visible light do not offer a case for scanning anyway, if inspection under people's clothes is pursued). Thus, less 'dense' information is acquired than could be done with X-rays. While X-rays are thought to be more dangerous in a generic way, they are also possible to apply at very low levels of radiation, such that the ensuing danger will be found acceptable by many (which is the configuration in which X-ray technologies are actually deployed in the United States, among others). It is largely because of public concern that in Europe, X-rays are abandoned in favour of millimetre-wave technologies. Thus, what seems to be a merely technical choice for a particular frequency band, is at closer look to a considerable extent a political, discursive choice as well.

This might appear as an unfortunate technical choice that is enforced by social circumstances: only poor pictures can be made because the public rejects a technologically superior alternative. But there is a bit more to say about it. In fact, the possibility to only render bodies in a less detailed way is a benefit when it comes to protecting privacy. As an interviewee from one vendor explains, while this less dense information may seem a mere downside, it is being used by them in an ingenious manner. The mm-wave data collected by their particular device is informationally too austere to actually create a photograph-like picture. The device is unable to make a picture, nor does it need to do so. Instead, it uses signal processing techniques to make the security assessment directly from the 'raw' sensor data. The impossibility of creating an image is in this case advertised as a privacy advantage over other systems. It thus clearly distinguishes from other *active millimetre wave scanner* technologies, which actually do internally produce a picture and then apply object recognition to it. Even though a picture created by the latter version does not look much like a photograph, it is still a representation of the body that might be felt to be a privacy encroachment. And even if this implicit picture is quite a few steps away from a naked photograph, it is still more of a privacy encroachment than having no potential to make picture at all.

What the analysis so far shows is that privacy and security as they appear in the end, are made up of a range of constituent factors. 'Security as inspection of a body while eliminating body details so as to preserve privacy' is not just that, but a very particular arrangement of technologies and operational procedures, and contingent on natural phenomena as well as technological states of the art. Also, many political and operational choices – which are not further attended to at this point – produce contingencies in the process of development, while themselves being equally contingent on other contextual factors.

This is what the notion of translation captures: not only are things connected and thereby somehow made present across multiple places, think for example of the assumed 'normal body' that is made present on the security work floor where it in effect constructs particular persons as abnormal; things are also themselves modified: the assumed normal body is itself modified under influence of what exactly is possible in terms of technological possibilities.

This entails, first, that problematic ‘anomalies’ as described with stoma patients are not easily resolved by ‘simply’ installing a different technology. This would incur a new classification scheme with its own anomalies. These anomalies might be different and even preferable for whatever reason, but there will fundamentally exist anomalies. Second, it entails that even though security gains and privacy losses are visible, this is by no means a trade-off between simple concepts in the sense I started this paper with. Even looking at the level of elements that make up privacy and security, it is not quite easy to explain how a “zero sum” between them is in place. Privacy and security are complex concepts, and indeed too complex to be thought of as standing in a relation as simple as a trade-off. As we will see shortly, though, it remains sensible to speak of a trade-off in very specific perspectives.

The emphasis so far on contingencies and complexities is not meant to argue, in any *technological determinist* vein, that the machine simply had to be developed this way. Rather, it is to argue that the complex network of relations that forms the basis of the machine, produces through its extensiveness a large degree of rigidity. While it is not fundamentally impossible to arrive at a different scanner, it will at least be very hard in practice, especially once certain choice are made and consolidated by implementation. It is also important to note that for this reason, it is not straightforward that security and privacy can easily be promoted at once, as for example the doctrine of *Privacy by Design* (henceforth PbD)[21] would have it.

Yet, this can also be carried in a slightly different direction. Looking at the airport security scanner once more, trade-offs become apparent in ways somewhat more complicated than a simple discursive trick to arrange people into particular disciplining ways. True enough, it could to some extent be expected beforehand that the classification by the AMS would put bomb-belt terrorists and people with a colostomy in the same ‘suspect’ category. This holds equally for technologies such as walk-through metal detectors and even for a manual pat-down. But it needs remembering here that millimetre-wave scanners were originally presented as a solution to exactly this problem. Yet, al that went into developing this particular scanner, i.e. the considerations of operational aptitude and matters of health safety etc., as well as the technical particularities, shows that that in the end, little more choice was left than accepting or not accepting the package deal of a particular added value for security and a particular privacy encroachment. Some privacy *is* traded in the end for security. However, what matters here is not this small observation, but the fact that particular technological choices entail a particular version of exactly *how* a particular privacy and a particular security are pitted against each other.

[21] Ann Cavoukian, *Privacy by Design: The 7 Foundational Principles* (Toronto, Ontario, Canada: Information and Privacy Commissioner of Ontario, 2009).

10.3 The Need for Interventional Models

The previous section has explained how the trade-off model in general falls short of explaining the intricacies of the versions of privacy and security that are produced in practice, even though some trade-off-like mechanisms are visible at a more detailed level of analysis. Yet, there is more that we may use models for than only providing an account or explanation of reality. The point is now to find uses of the trade-off model that are not, or at least not fatally, dependent on its empirical accuracy. In this context, it is also important to tap into the aforementioned apparent attractiveness (if not ineradicability) of the model in policy discourse: if you can't beat them, join them; and try to harness the impetus the model carries. The model is not only attractive as a rhetorical strategy, but apparently it manages to attract an entire discourse that naturally acquires momentum in policy making. This section and the one following it develop how it is possible, after taking warning from the external critiques discussed above, to use the trade-off model in legitimate ways.

One use in the sphere of policy making has already been hinted at. If a decision is pending, it is key to narrow down the factors that will be taken into account. As soon as issues that pertain to a decision become sufficiently large in number – as they mostly do in real-life situations – the decision-making process is no longer particularly eased by offering the completest possible account. Instead, a simpler take on the problem is more likely to acquire momentum.

I assume for the sake of argument that policy typically centres on propositional questions, that is questions that can be answered in comparably unambiguous terms. By this simplification, I bypass the whole debate on whether policy can, should or actually does limit itself to such propositional questions,[22] but the simplification is in this case empirically legitimized by the very persistence of uses of variants of the trade-off model in policy contexts. In face of this need for propositional questions, the trade-off model offers an interesting potential.

Policy typically takes some near future as its object, whereas many translations in the sense discussed before become visible first in the process of implementation. Over thirty years ago, Collingridge posited a dilemma in the social control of technology: in early stages of development, when change is comparably easy and affordable, the need for it is hard to recognize; later, when the need becomes apparent, it will have become harder and more costly because of costs and interdependencies that are sunk into the development process.[23] Even though Collingridge at his time built an argument in a rather a-political way about big technoscientific projects, we can still easily generalize his argument to political and moral issues,

[22] Harry M. Collins and Robert Evans, "The Third Wave of Science Studies," *Social Studies of Science* 32, no. 2 (2002); Brian Wynne, "Seasick on the Third Wave? Subverting the Hegemony of Propositionalism: Response to Collins and Evans (2002)," ibid. 33, no. 3 (2003); Sheila Jasanoff, "Breaking the Waves in Science Studies: Comment on H.M. Collins and Robert Evans, 'the Third Wave of Science Studies'," ibid.

[23] David Collingridge, *The Social Control of Technology* (New York: St.-Martin's Press, 1980).

and state that in early phases of the development particular effort must be made to surface issues that might occur later.

Given its upstream position, policy rightfully has a preference for more abstract and generic approaches, and it merits exploration whether simplifying models such as the trade-off model can deliver that. Of course, alternatively, it could be argued that methods have been sufficiently developed to supply the information that is needed at upstream locations. Methods such as technology forecasting and technology assessment may produce a rich account of the technology-in-practice as it may emerge at some point. However, it is not always best to inform policy decisions with a complete account of the complexity of practices. Quite the contrary, policy needs some simplification as this is the only way to achieve generalization, rather than having to issue a new policy for each new situation.

This need for simplification is exactly why principles such as the ones specified by *Privacy by Design* find resonance. The guidelines of PbD are clear with respect to what should be pursued through technological design. Privacy should be integral to the design, a default mode intrinsically connected to it, rather than something that is fitted in *post hoc* when the design is largely completed. At the same time, the doctrine of PbD has been argued to pay insufficient attention to the difficulties that implementing such principles confront. For example, it needs restructuring of entire industries, including much more bottom-up processes where solutions are now often modularly made up of existing elements.[24] Also, it has been argued that the PbD doctrine is insufficiently specific, and could easily be mistaken for a simple problem that is to be solved with a checklist.[25] Finally, the process itself of shifting implementations towards a stronger intrinsic connection with privacy requires a reallocation of resources, which implies a trade-off of at some level, as these resources will have to come from somewhere. The notion of win-win situation is a marketing invention, not an unproblematic reality that can be picked off the shelf.

These comments reflect that the 30-year old Collingridge dilemma has not lost all of its topicality. The changes required by important principles are fundamentally difficult to operationalize as they are quite some steps of translation away from the actual context of operation. There is insufficient knowledge about the eventual shape of technologies, and in particular the ways important values are translated into those technologies as was touched upon in the previous section. Thus, the Collingridge dilemma reappears here as largely an epistemic catch-22, and a fundamentally unresolvable one at that. In regard of this difficulty, in combination with the aforementioned propositional questions, questions in trade-off style might exactly offer a simplification that is needed to connect the policy context with the eventual sociotechnical context of operation.

[24] Sarah Spiekermann, “Viewpoint: The Challenges of Privacy by Design,” *Communications of the ACM* 55, no. 7 (2012).

[25] Seda F. Gürses, Carmela Troncoso, and Claudia Diaz, “Engineering Privacy by Design,” *Computers, Privacy & Data Protection* (2011).

As mentioned in the beginning, the internal critique holds that the trade-off model inaccurately describes reality. The sociotechnical analysis added further complexity in support of the claim that a simple account such as the trade-off model is not tenable. However, with the external points of critique, things are a bit more complicated. To some extent, the tenability of external critiques is dependent on the internal critique: if facts are misrepresented, then anything we do with them cannot be much either. Because of its empirical inaccuracy, the trade-off model disqualifies as a justification for imposing privacy-encroaching security measures.

However, not everything that – legitimately – happens in discourse, is dependent on the most accurate and elaborate representation of facts. Indeed, the Collingridge dilemma and its marginal elaboration above show that it is at some points impossible work on the basis of clear facts, simply because clear facts are not there (which is a rather different problem than the intrinsic contestability that renders politically relevant facts unstable, which is not further developed here). From the sociotechnical complexities articulated in the previous section, some conclusions can be drawn about how it can offer some solace to the epistemic difficulties subsumed under the Collingridge dilemma.

10.4 How to Use the Trade-Off Model

What we have so far is the observation that the trade-off model is empirically problematic, but nonetheless successful in attaining impetus in policy-making discourses. The question thus is how use of a trade-off model can be shaped in a way that appears legitimate, while it also takes account of the critique that was presented and extended by the sociotechnical empirical analysis. In particular, the use must be such that no false choices are imposed on the public by appeal to the trade-off model. In second instance, if such use is generally found, it might also be able to provide an alternative to the oversimplification that was discerned in PbD.

For one thing, the sociotechnical analysis articulates the subjects that privacy and security refer to. In this case, just as in the general case, these are not be the same: the person whose privacy is sacrificed may be a very different person than the one whose security is increased. Indeed, in this case, some someone's privacy is traded off against somebody else's security: the privacy of stoma patients is given up in return for some idea of safety, understood as liquids being kept out of airplanes. While this is only one part of the story, and while the whole story still cannot be captured in trade-off terms, this small part can. The analysis shows that sociotechnical arrangements may produce a *displacement*: two sides of a balance may be mediated by extensive chains of translation.

This hints at one particular use of the trade-off model: it might serve to identify such displacements. Rather than putting on the agenda a question like 'do we want privacy or do we want security', the question should be asked: 'given that this security option is available, which privacy does it sacrifice for which security?'

This mobilizes the trade-off model with all of its simplicity as a heuristic in support of exactly the propositional questions that are attractive to policy discourses. It helps identifying stakeholders and their interests.

Second, the sociotechnical analysis articulated many of the elements that go into the eventual ways privacy and security are performed. In much the same way the interests of stakeholders are possible to articulate by asking trade-off-like questions, the trade-off model can serve to discuss relations between particular *elements*, or between particular alternatives of translations. For example, in this case it might be asked at an early stage of developing the AMS what exactly the security benefits are, and what the relative security costs would be for further privacy. In this case the privacy costs could have been identified by looking more closely at the exact definitions of anomalies, and the trade-off heuristics would have helped articulating that in fact this privacy problem is rather 'orthogonal' to security, rather than mutually exclusive. Parts of the sociotechnical configuration could be interrogated as to the matter of how they connect to both privacy and security. This should then be the starting point of inquiry, not a conclusive model. Such a strategy is immune to the kind of external critiques identified above.

At this point, yet another clear strategy deploying a trade-off model starts to appear: it urges to investigate where the costs – in a wide sense, including social costs – of a particular conception of security go. In this case, this would clearly have helped articulating the problem with stoma patients. For initially, the scanner was presented as a security device with *no* costs for privacy, since the mannequin representation arguably contains no private information. However, inquiring after the privacy costs, which according to a strict-sense trade-off model inevitably occur, would potentially have sensitize discussants towards the *displaced* privacy costs for colostomy patients. Even if privacy and security are not fundamentally at odds, they may in the end be implemented in such a displacing way, and it never hurts to use a trade-off model as a heuristic, and use it to try and find downsides of an implementation that would otherwise remain hidden as a result of the particular perspective chosen.

Using the trade-off model as a heuristic rather than as a representational model also precludes another external critique, the misleading – and hitherto dominant – justificatory use of the trade-off model. It makes similar sense to substitute a heuristic use of the trade-off model for its hitherto dominant justificatory use. For example, the critique that public perceptions do not reflect an understanding of reality in terms of a trade-off model[26] can be circumvented by using the trade-off model as a heuristic to probe how the public conceives of privacy and security issues. If the public indeed sees privacy and security in a more complex relation than a trade-off, it might still be asked, with the sociotechnical complexities in mind, which connections they *do* see between privacy and security. Indeed, as the sociotechnical analysis shows, there actually are trade-offs between very specific constituent

[26] Pavone and Esposti, "Public Assessment of New Surveillance-Oriented Security Technologies: Beyond the Trade-Off between Privacy and Security."

parts of security and privacy, but they are mediated by chains of sociotechnical translations. These translations are what ought to be articulated through the use of the trade-off model. And then, it may still make sense to see and discuss these connections in terms of costs and benefits, without assuming a simple trade-off between privacy and security at large. The trade-off model is then again just one method of getting there.

Finally, the critique that the trade-off typically appears as a vague but great risk which trumps less urgent notions of privacy can be used discursively to reverse the burden of proof: if you want me to sacrifice this part of my privacy, then please further explain the urgency of the security threat, and how sacrificing my privacy actually helps coping with the threat. The abovementioned business card in the chest pocket will in general not be particularly privacy sensitive, but that does not render any less legitimate the question of how security is served by taking the business card out of the private sphere. It may in this particular case shed different light on the proportion of the privacy encroachment.

This reversal is vital: whereas Chandler[27] suggests we should ask how privacy-reducing (sic) measures reduce security because that kind of inquiry makes sure that appropriate values are pitted against each other, it is probably easier to gain discursive support for a strategy that resonates well with the persistent trade-off model. For that matter, the proposed reversal of the burden of proof could also be phrased as a demand to show how a particular promotion of privacy poses a threat to security. The sociotechnical analysis shows that in a particular (whether envisioned or existing) configuration, indeed some trade-off like relations become inevitable (where inevitable refers to an emerging necessity in view of specific circumstances, not a fundamental impossibility in a more abstract sense).

10.5 Conclusions

This paper commenced by dissecting the critique of the trade-off model into internal and external critiques. The internal critique, to which the sociotechnical analysis performed here even added, is largely tenable. However, separating the internal from the external critique shows that the external critique so far mainly concerns the use of the trade-off model in justification of privacy encroachments, which is indeed questionable insofar as it would depend on factual accuracy. However, in this paper, it was shown that this justificatory use is just one of many possible, and that heuristic uses can be defended convincingly.

To the light of the sociotechnical analysis, the call by Schneier[28] that the trade-off model be abandoned in its entirety to regain the choice to have 'both privacy and

[27] Chandler, "Privacy Versus National Security: Clarifying the Trade-Off."

[28] Schneier, "Protecting Privacy and Liberty. The Events of 11 September Offer a Rare Chance to Rethink Public Security."

security' rather than being deprived of privacy by a false appeal to security seems a bit too easy. The same holds of course for (uncritical interpretations of) the *Privacy by Design* doctrine. It is still virtually impossible to develop a technology that will satisfy all interests, witness the complexities articulated in the sociotechnical analysis. However, while leaving much of the internal and external critiques intact, the trade-off model can even help us to arrive at a more nuanced way of debating. As a heuristic, the trade-off model can help to unite and organize 'hybrid forums' where heterogeneous collectives of actors discuss technological options.[29] In such forums, the model may help internalizing effects that would otherwise continue to be understood as externalities – specifically, it helps internalizing privacy in the design process, rather than accepting it as an external cost that is to be accepted for the sake of security.

True enough, the proposed use of the trade-off model is not *exactly* the simplification that was suggested in the beginning as needed by policy. In fact, the whole operation chiefly answers the call by Wynne that policy making requires much more than merely answering propositional questions, notably that it also needs to address in a discursive way the meanings of terms and concepts in which the very propositional questions are couched.[30] Indeed, the suggestions made so far in this paper do offer a gradient towards such a discursive and intersubjective approach to the meaning of concepts. However, the trade-off model itself remains a simple device and is thereby likely to gain more momentum than, say, inviting a philosopher into the policy room. The model is at the same time down-to-earth and sufficiently controversial to fulfil exactly this task.

Regarding the question why the trade-off model is an appropriate avenue to go down, and not any other model, the answer is utterly pragmatic: the trade-off model is attractive because it is found to be attractive (and perhaps even convincing) by people who matter in the policy-making process. More specifically, the model is popular among people who are *in control* of such decision processes. Much like a judoka deflects the force and impetus of an attacker to floor the very attacker, the impetus of the trade-off model could be used to break dominant discourses that use that very model to legitimize privacy encroachments.

Acknowledgements The empirical research underlying this paper was made possible by the ERC 7th Framework Programme, and was part of the PRISMS project (FP7-SEC-2010-285399, www.prismsproject.eu). An early version of the paper was presented and discussed during the *Computers, Privacy and Data Protection 2014* conference. The author wishes to thank the volume editors and two anonymous reviewers for their valuable feedback.

[29] Michel Callon, Pierre Lascoumes, and Yannick Barthe, *Acting in an Uncertain World: An Essay on Technical Democracy* (Cambridge MA: The MIT Press, 2009).

[30] Wynne, "Seasick on the Third Wave? Subverting the Hegemony of Propositionalism: Response to Collins and Evans (2002)."

Bibliography

Akrich, Madeleine, and Bruno Latour. "A Summary of a Convenient Vocabulary for the Semiotics of Human and Nonhuman Assemblies." In *Shaping Technology, Building Society: Studies in Sociotechnical Change*, edited by W. E. Bijker and J. Law, 259–64. Cambridge, MA: MIT Press, 1992.

Amoore, Louise. "Biometric Borders: Governing Mobilities in the War on Terror." *Political Geography* 25, no. 3 (2006): 336–51.

Callon, Michel. "Some Elements of a Sociology of Translation: Domestication of the Scallops and the Fishermen of Saint Brieuc Bay." In *Power, Action and Belief: A New Sociology of Knowledge?*, edited by John Law, 196–233. London: Routledge and Kegan Paul, 1986.

Callon, Michel, Pierre Lascoumes, and Yannick Barthe. *Acting in an Uncertain World: An Essay on Technical Democracy*. Cambridge MA: The MIT Press, 2009.

Cavoukian, Ann. *Privacy by Design: The 7 Foundational Principles*. Toronto, Ontario, Canada: Information and Privacy Commissioner of Ontario, 2009.

Chandler, Jennifer. "Privacy Versus National Security: Clarifying the Trade-Off." Chap. 7 In *On the Identity Trail: Anonymity, Privacy and Identity in a Networked Society*, edited by Ian Kerr, Valerie Steeves and Carole Lucock, 121–38. Oxford: Oxford University Press, 2009.

Collingridge, David. *The Social Control of Technology*. New York: St.-Martin's Press, 1980.

Collins, Harry M., and Robert Evans. "The Third Wave of Science Studies." *Social Studies of Science* 32, no. 2 (2002): 235–96.

Davis, Darren W., and Brian D. Silver. "Civil Liberties Vs. Security: Public Opinion in the Context of the Terrorist Attacks on America." *American Journal of Political Science* (2004).

Euronews. "Obama Defends 'Privacy Trade-Off' for Security." http://www.euronews.com/2013/06/07/obama-defends-privacy-trade-off-for-security/.

Finn, Rachel L., David Wright, and Michael Friedewald. "Seven Types of Privacy." In *European Data Protection: Coming of Age*, edited by Serge Gutwirth and Yves Poullet. Dordrecht: Springer, 2013.

Gaskell, George, Nick Allum, Wolfgang Wagner, Nicole Kronberger, Helge Torgersen, Juergen Hampel, and Julie Bardes. "Gm Foods and the Misperception of Risk Perception." *Risk Analysis* 24, no. 1 (2004).

Gürses, Seda F., Carmela Troncoso, and Claudia Diaz. "Engineering Privacy by Design." *Computers, Privacy & Data Protection* (2011).

Jasanoff, Sheila. "Breaking the Waves in Science Studies: Comment on H.M. Collins and Robert Evans, 'the Third Wave of Science Studies'." *Social Studies of Science* 33, no. 3 (2003): 389–400.

Latour, Bruno. *Science in Action - How to Follow Scientists and Engineers through Society*. Cambridge MA: Harvard University Press, 1987.

Law, John. "Actor Network Theory and Material Semiotics." In *The New Blackwell Companion to Social Theory*, edited by Bryan S. Turner, 141–58. Chichester: Blackwell, 2009.

Law, John. *After Method: Mess in Social Science Research*. London, New York: Routledge, 2004.

Law, John, and John Urry. "Enacting the Social." *Economy and Society* 33, no. 3 (2004): 390–410.

Lieshout, Marc van, Michael Friedewald, David Wright, and Serge Gutwirth. "Reconciling Privacy and Security." *Innovation: The European Journal of Social Science Research* 26, no. 1–2 (2013): 119–32.

Movius, Lauren B. "U.S. And Eu Privacy Policy: Comparison of Regulatory Approaches." *International Journal of Communication* 3 (2009): 169–87.

Pavone, Vincenzo, and Sara Degli Esposti. "Public Assessment of New Surveillance-Oriented Security Technologies: Beyond the Trade-Off between Privacy and Security." *Public Understanding of Science* 21, no. 5 (July 1, 2012): 556–72.

Schneier, Bruce. "Protecting Privacy and Liberty. The Events of 11 September Offer a Rare Chance to Rethink Public Security." *Nature* 413, no. 25 October 2001 (2001).

Solove, Daniel J. ""I've Got Nothing to Hide" and Other Misunderstandings of Privacy." (2007).

Solove, Daniel J. *Nothing to Hide: The False Tradeoff between Privacy and Security*. New Haven, London: Yale University Press, 2011.

Spiekermann, Sarah. "Viewpoint: The Challenges of Privacy by Design." *Communications of the ACM* 55, no. 7 (2012): 38–40.

Strickland, Lee S., and Laura E. Hunt. "Technology, Security, and Individual Privacy: New Tools, New Threats, and New Public Perceptions." *Journal of the American Society for Information Science and Technology* 56, no. 3 (2005): 221–34.

Warren, Samuel, and Louis D. Brandeis. "The Right to Privacy." *Harvard Law Review* 193 (1890).

Wright, David, Serge Gutwirth, Michael Friedewald, Paul De Hert, Marc Langheinrich, and Anna Moscibroda. "Privacy, Trust and Policy-Making: Challenges and Responses." *Computer Law & Security Review* 25, no. 1 (2009): 69–83.

Wynne, Brian. "Seasick on the Third Wave? Subverting the Hegemony of Propositionalism: Response to Collins & Evans (2002)." *Social Studies of Science* 33, no. 3 (2003): 401–17.

Chapter 11
Privacy and Security – On the Evolution of a European Conflict

Matthias Leese

Abstract Privacy and security have long been framed as incommensurable concepts that had to be traded off against each other. While such a notion is rather under-complex, it has been quite persistent. In recent years, however, the relation has undergone a transformation and is now apparently conceived of as a technological issue that is set to be resolved through privacy by design. This paper retraces, through an analysis of EU security research funding, how this shift has come about, and critically assesses its potential to eventually resolve the conflict between privacy and security in a world of data-driven security measures.

Keywords Security • Privacy • Research • Horizon 2020 • European Union

Privacy and security have often been framed as conflicting concepts that must be conceived of as incommensurable and thus constitute a trade-off.[1] And although such a notion has been largely criticized for using under-complex definitions of both privacy and security, as well as for neglecting empirical examples of positive sum games and questions of whose privacy and whose security are affected,[2] the trade-off model appears quite persistent. Considering the contemporary nature of data-driven security measures, much digital ink has been spilled about the presumably weak standing of privacy in the face of a more or less overwhelming context of (inter-)national security.[3] This paper analyzes how the relation between privacy and

[1] Marc van Lieshout et al., "Reconciling Privacy and Security," *Innovation: The European Journal of Social Science Research* 26 (2013).

[2] Govert Valkenburg. "The Trade-Off Model Between Privacy and Security From a Sociotechnical Perspective. Paper presented at Computers, Privacy and Data Protection Conference, Brussels, 22–24 January." 2014.

[3] see for instance Colin J. Bennett, "What Happens When You Book an Airline Ticket? The Collection and Processing of Passenger Data Post-9/11," in *Global Surveillance and Policing. Borders, Security, Identity*, ed. Elia Zureik and Mark B. Salter (Cullompton/Portland: Willan,

M. Leese (✉)
University of Tuebingen, Tübingen, Germany
e-mail: matthias.leese@izew.uni-tuebingen.de

S. Gutwirth et al. (eds.), *Reforming European Data Protection Law*,
Law, Governance and Technology Series 20, DOI 10.1007/978-94-017-9385-8_11

security has been framed and re-framed in the field of European security research, eventually ending up as a question of privacy by design. Privacy by design, so the argument goes, enables new security technologies to be both privacy-preserving as well as effective and efficient, and thus would ultimately serve as the silver bullet that resolves the conflict/trade-off. However, this paper puts forward the claim that the notion of privacy by design rather puts old wine into new bottles, as a closer look reveals that the core problem is not tackled, but only re-framed according to the general technical scope of security research. Thus, it appears that the new emphasis on privacy and the ensuing argumentative mitigation of the conflict merely intends to comply with the EU's increased focus on normative security and at the same time renders research governance as a technological fix for the technological fix that security is conceptualized as in the first place.

The paper proceeds by providing a brief overview of the emergence of security research at the EU level over the last decade and sheds light on its underlying rationalities, *en passant* retracing how the presumed trade-off between privacy and security was framed and eventually evolved into a privacy by design approach alongside the emergence of a more normatively coined EU 'security project'. The paper concludes with a critical assessment that questions the suitability of privacy by design as the panacea that it comes advertised as.

11.1 EU Security Research – On the Emergence of a Field and a Conflict

"Security research is the new guy in town."[4] As opposed to 'traditional' fields of research funded by the European Union, research that is explicitly dedicated to the security of the EU and its citizens has only been around for the relatively short term of about a decade,[5] and has at times struggled to find its niche among related fields with a strong 'security touch', such as for instance Information and Communication Technologies (ICTs). However, fostered by 'new' and global threat scenarios,

2005); Matthias Leese, "Blurring the Dimensions of Privacy? Law Enforcement and Trusted Traveler Programs," *Computer Law & Security Review* 29 (2013); Helen Nissenbaum, *Privacy in Context: Technology, Policy, and the Integrity of Social Life* (Stanford: Stanford Law Books, 2010); Anastassia Tsoukala, "Risk-focused Security Policies and Human Rights. The Impossible Symbiosis," in *Mapping Transatlantic Security Relations. The EU, Canada, and the War on Terror*, ed. Mark B. Salter (London/New York: Routledge, 2010).

[4] J. Peter Burgess. "Ethical Review and the Value(s) of Security Research." Paper presented at the Workshop Ethical Issues in Security Research – a Practical Approach, Brussels, 29 September, 2011.

[5] Ibid.; ECORYS. "Study on the Competitiveness of the EU Security Industry. Within the Framework Contract for Sectoral Competitiveness Studies – ENTR/06/054: Final Report." 2009; Didier Bigo and Julien Jeandesboz. "The EU and the European Security Industry: Questioning the 'Public-Private Dialogue'. INEX Policy Brief No. 5." 2010.

the quest for appropriate remedies has become an integral part of the realm of fundamental and applied research that is set to produce new tools and technologies, and thus to contribute to effectively establishing security in the European Union – or so the argument goes. Arguably, the need for reinforced security solutions has been catalyzed by the debate that was kindled by the events of 9/11 and their massive aftermath in terms of security policy adjustments.[6] In the EU, security is now conceived of as a cross-cutting concept that has to tackle widespread areas such as terrorism, serious and organised crime, cybercrime, cross-border crime, violence itself, and natural and man-made disasters.[7] Thus, security research has eventually been established as a key area within the European funding framework.

This very framework, however, is currently undergoing structural change. In 2014, EU research funding has hit an institutional threshold as the established Framework Programmes (FP) come to an end with FP7 and will be replaced by an overhauled, streamlined, and arguably simplified and more efficient program entitled Horizon 2020.[8] Official documents promise that this new framework will, amongst other, set clearer scopes on societal issues, most notably privacy and data protection.[9] Thus, this structural change appears an appropriate break to analyze how the still emerging field of security research is being (re-)shaped alongside economic rationalities and the emergence of a European 'security project' itself, and how the relationship between privacy and security keeps evolving. In order to set out an analytical framework, this paper argues that EU security research funding follows two general trajectories: it is mainly conceived of as (1) a means to foster the European economy, and (2) as a primarily technical framework that aims to produce specific solutions to clearly defined security problems. In recent years, however, a third notion has been added to this dichotomy, as 'security' itself is now increasingly presented as a normatively embedded concept that needs to comply with human rights and civil liberties. This appears to be a major reason for abandoning the trade-off model and the search for new and integrative approaches, eventually ending up with privacy by design.

'Historically' speaking, EU security research can be framed as a field that has been shaped through an inextricable entanglement with the industrial sector, as

[6] It should be noted, however, that the notion of a post-9/11 'break' in terms of security policy has been contested such that recent developments should rather be seen as part of a larger historical trajectory. See David Lyon, "Airports as Data Filters: Converging Surveillance Systems after September 11th," *Journal of Information, Communication and Ethics in Society* 1 (2003).

[7] European Union. "Internal Security Strategy for the European Union: Towards a European Security Model." 2010, 14–16.

[8] For an overview of Horizon 2020, see http://ec.europa.eu/programmes/horizon2020/ (last accessed 26 February 2014).

[9] European Commission. "Commission Staff Working Paper. Impact Assessment. Accompanying the Communication from the Commission 'Horizon 2020 – The Framework Programme for Research and Innovation'." SEC(2011) 1427 final, 30 November, 2011.

has been compellingly shown by Bigo, Jeandesboz, Hayes, and others.[10] Multiple companies and personalities from the branch have been involved in setting up of the field and the intensified cooperation between the Commission and the industry, taking off in 2003 with the establishment of the *Group of Personalities in the Field of Security Research* (GoP)[11] and the initiation of the *Preparatory Action on Security Research* (PASR) in 2004. The GoP was eventually followed up by the *European Security: High Level Study on Threats, Responses and Relevant Technologies* (ESSTRT) in 2006[12] and the setting up of the *European Security Research Advisory Board* (ESRAB)[13] in 2005 and the *European Security Research Innovation Forum* (ESRIF)[14] in 2008, both of which further envisioned the future of security research at the EU level.

Throughout the published reports of the aforementioned fora, particularly privacy and data protection have been framed as disruptive elements for security technologies and thus for the overall goal of a secure European Union. For instance, as Bigo and Jeandesboz have pointed out, the ESSTRT final report frames the conflict such that "the underlying assumption is that intrusiveness is a requirement for efficiency, and that privacy undermines efficiency",[15] and the ESRAB report states that "research into ethics and privacy, and the trade-off between improved security and loss of privacy, will influence technology development and in parallel address aspects of how citizens perceptive security and insecurity."[16] Thus, privacy and security were generally conceived of as incommensurable concepts, and it was very clear where the preferences for effective security research had to be placed – the need for security apparently trumped the need for privacy. Either security measures would work, and this would be because they would be based on a sufficiently large database that allowed for glimpses of the future and the next event that needs to be

[10] Bigo and Jeandesboz, "The EU and the European Security Industry: Questioning the 'Public-Private Dialogue'. INEX Policy Brief No. 5."; Ben Hayes, *NeoConOpticon. The EU Security-Industrial Complex* (Amsterdam: Transnational Institute/Statewatch, 2009); Ben Hayes, *Arming Big Brother: The EU's Security Research Programme* (Amsterdam: Transnational Institute/Statewatch, 2006).

[11] Group of Personalities in the Field of Security Research. "Research for a Secure Europe. Report of the Group of Personalities in the Field of Security Research." 2004.

[12] European Security: High Level Study on Threats Responses and Relevant Technologies. "Deliverable D6-1 (Final Report): New European Approaches to Counter Terrorism, 21 March." 2006.

[13] European Security Research Advisory Board. "Meeting the Challenge: the European Security Research Agenda. A Report from the European Security Research Advisory Board." 2006.

[14] European Security Research & Innovation Forum. "ESRIF Final Report, available at http://ec.europa.eu/enterprise/policies/security/files/esrif_final_report_en.pdf (last accessed 26 February 2014)." 2009.

[15] Bigo and Jeandesboz, "The EU and the European Security Industry: Questioning the 'Public-Private Dialogue'. INEX Policy Brief No. 5," 6.

[16] European Security Research Advisory Board, "Meeting the Challenge: the European Security Research Agenda. A Report from the European Security Research Advisory Board," 8.

canceled out – or they wouldn't work because privacy claims and the restrictions of the data protection framework would thwart their effectiveness. More or less independent of any actual conceptualizations of privacy, be it as the classical "right to be left alone"[17] that entails a "boundary control process",[18] as the "claim of an individual to determine what information about himself of herself should be known to others"[19] which in terms involves "a constraint on the use of power",[20] or politically as the foundation of the democratic constitutional state[21] – any position that values the (digital) personal sphere would be considered disruptive from an industry point of view. Especially when taking into consideration Helen Nissenbaum's concept of privacy in context,[22] one might indeed be inclined to say that threat scenarios were used to create a contextual override for privacy arguments.

As mentioned earlier, such a trade-off model is certainly oversimplified, and arguably only represents a part of the full story. How come we find such a striking neglect of privacy arguments in official documents, then? The next section aims at unpacking the underlying notions of security and security research in the European Union. It will become clear that EU security research unfolds along a clear-cut economic agenda, and thus introduces a very specific and market-driven approach to the relationship between privacy and security.

11.2 Economics and Technologies

First trajectory. Both FP7 and Horizon 2020 documents acknowledge the economic goals identified by the Europe 2020 strategy,[23] framing "research and innovation as central to achieving the objectives of smart, sustainable and inclusive growth."[24] The underlying rationale, as stated by the Staff Working Paper on Horizon 2020, is

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

[18] Irwin Altman, "Privacy Regulation: Culturally Universal or Culturally Specific?," *Journal of Social Issues* 33 (1977): 67.

[19] Alan F. Westin, "Social and Political Dimensions of Privacy," *Journal of Social Issues* 59 (2003): 431.

[20] Priscilla M. Regan, "Response to Bennett: Also in Defence of Privacy," *Surveillance & Society* 8 (2011): 498.

[21] Michael Friedewald et al., "Privacy, Data Protection and Emerging Sciences and Technologies: Towards a Common Framework," *Innovation: The European Journal of Social Science Research* 23 (2010): 62.

[22] Nissenbaum, *Privacy in Context: Technology, Policy, and the Integrity of Social Life*.

[23] European Commission. "Communication from the Commission. Europe 2020: A strategy for Smart, Sustainable and Inclusive Growth." COM(2010) 2020 final, 3 March, 2010.

[24] European Commission. "Proposal for a Regulation of the European Parliament and of the Council Laying Down Rules for the Participation and Dissemination in 'Horizon 2020 – the Framework Programme for Research and Innovation (2014–2020)'." COM(2011) 810 final, 30 November, 2011, 2.

that "modern economic theory unanimously recognises that research and innovation are prerequisites for the creation of more and better jobs, for productivity growth and competitiveness, and for structural economic growth."[25] For that purpose, a study on behalf of DG Industry & Enterprise has analyzed the global security market and the position of the European security industry, coming to the conclusion that "it appears vital to stimulate and create a proper innovation framework in the security domain and establish fast track development procedures for new market technology requirements."[26] As a consequence from those findings, the European Commission in 2012 adopted an "Action Plan for an innovative and competitive Security Industry"[27] in order to secure and extend market shares in a rapidly growing global security economy.

In the same year, the Commission published a document on EU security research entitled "Safeguarding Society, Boosting Growth."[28] Overlooking its content, it quickly becomes clear that the emphasis lies on the latter part, as the document states that

> our objective, notably through our Security Industrial Policy initiative, is to improve the global competitiveness of the EU security industry by stimulating its growth, invest in the research and development of future, world-leading security technologies and processes, and launch any effort necessary to overcome the current market fragmentation for security products in the EU and thus establish a true Internal Market.[29]

In fact, the conceptualization of EU research funding as a policy tool for economic growth has always been out in the open. Particularly, the purpose of security research can be identified by its institutional location. The housing within DG Enterprise and Industry instead of the maybe more natural fit DG Research & Innovation indeed provides a clear statement and has been criticized for its "significant consequences for the way we understand and do research on security as an ethically charged field of research."[30] This general economic scope will likely be reinforced with the start of Horizon 2020. As the joint communication on the new framework states, "since the launch of the Seventh Framework Programme (FP7), the economic context has changed dramatically",[31] and now urges the EU to

[25] European Commission, "Commission Staff Working Paper. Impact Assessment. Accompanying the Communication from the Commission 'Horizon 2020 – The Framework Programme for Research and Innovation'," 7.

[26] ECORYS, "Study on the Competitiveness of the EU Security Industry. Within the Framework Contract for Sectoral Competitiveness Studies – ENTR/06/054: Final Report," xvii.

[27] European Commission. "Communication from the Commission to the European Parliament, the Council and the European Economic and Social Committee. Action Plan for an Innovative and Competitive Security Industry." COM(2012) 417 final, 26 July, 2012.

[28] European Commission. "EU Security Research: Safeguarding Society, Boosting Growth." 2012.

[29] Ibid., 1.

[30] Burgess, "Ethical Review and the Value(s) of Security Research," 1.

[31] European Commission. "Communication from the Commission to the European Parliament, the Council and the European Economic and Social Committee and the Committee of the Regions.

provide even stronger incentives, since "research and innovation help deliver jobs, prosperity, quality of life and global public goods."[32]

The ECORYS report on the competitiveness of the European security industry bolsters those general assumptions with factual numbers. The global security market is estimated to be worth €100 billion, with the size of the European market in the range of €26 to €36.5 billion.[33] This translates into roughly 180,000 employees in the European security sector. Accordingly, security research receives a considerable amount of funding, with the security theme under the FP7 being worth an overall amount of €1.4 billion[34] and the financial terms for the "Secure Societies" action under Horizon 2020 alone determined at €1.7 billion. However, despite those efforts, the ECORYS report points out a "low aggregate level of EU funding for security-related research, technology development and innovation."[35] In a comparative perspective, EU security research funding still remains "considerably below the efforts made in the USA", leading to "potential weaknesses in the underlying competitiveness of the EU security sector."[36] This could in terms lead to a predicted loss of market shares to a low of 20 % in 2020,[37] particularly with the Asian security industry massively catching up in the high-tech area, but also with considerable competition from Russia and Israel.[38] The remedy for such a threatening scenario appears quite simple: reinforcement of market stimulation through enhanced security research funding and faster product cycles.[39] Thus, one might indeed be inclined to agree with Bill Clinton's famous statement that "it's the economy, stupid". Economic prosperity has been the driving force behind European integration from the beginning, and why should it change within security research, of all things?

The Action Plan for the security industry subsequently provides concrete steps of action in order to reinforce the competitiveness of the European security industry, suggesting the creation of a true Internal Market through favorable conditions, the enhancement of competition and lower production costs, as well as strengthened

Horizon 2020 – The Framework Programme for Research and Innovation." COM(2011) 808 final, 30 November, 2011, 2.

[32] Ibid.

[33] ECORYS, "Study on the Competitiveness of the EU Security Industry. Within the Framework Contract for Sectoral Competitiveness Studies – ENTR/06/054: Final Report," v.

[34] European Commission, "EU Security Research: Safeguarding Society, Boosting Growth," 2.

[35] ECORYS, "Study on the Competitiveness of the EU Security Industry. Within the Framework Contract for Sectoral Competitiveness Studies – ENTR/06/054: Final Report," x.

[36] Ibid., 38.

[37] European Commission, "Communication from the Commission to the European Parliament, the Council and the European Economic and Social Committee. Action Plan for an Innovative and Competitive Security Industry," 2.

[38] ECORYS, "Study on the Competitiveness of the EU Security Industry. Within the Framework Contract for Sectoral Competitiveness Studies – ENTR/06/054: Final Report," 51–60.

[39] Ibid., xvii.

support for SMEs.[40] Apart from those issues, however, one of the most pressing concerns still appears to be the potential of privacy and data protection to thwart the effectiveness of security technologies and thus their successful market impact in the first place. Subsequently, the Action Plan takes up on that conflict and states that a major problem arising from the societal dimension of security research is the social acceptance of security technologies – or rather the lack thereof, which could result in a number of negative consequences for the security industry, i.e. wasted investments.[41] Most strikingly, privacy requirements are regarded to hurt the security market on both supply and demand side. For the supply side (i.e. the European security industry), this would mean that its products might not reach their maximum 'security potential' due to constraints in data collection and analysis, and "for the demand side it means being forced to purchase a less controversial product which however does not entirely fulfill the security requirements."[42] Thus, from an industry angle, the situation appears quite clear: privacy hampers security. Or rather, it hampers security technologies, as EU security research is indeed primarily locked in on the emergence of new technologies.

Second trajectory. The rationale behind this scope becomes clearer when looking at how current security efforts within the EU are conceptualized as data-driven and risk-mitigating measures. As security policies increasingly emphasize the potential of databases, data-sharing and interoperability for the purpose of gathering knowledge and thus being able to prevent future risks,[43] Information and Communication Technologies (ICTs) have spilled over into security contexts – and with them issues of privacy (and data protection). Security technologies heavily focus on communication, social networks, and other forms of individual interaction with a digitized everyday environment, such as sensors or biometrics. The massive amount of personal and behavioral data constantly produced then serves as the basis for fighting crime and terrorism through various forms of data exploitation such as algorithmic profiling and probabilistic risk calculations.[44] Or, put more simply:

[40] European Commission, "Communication from the Commission to the European Parliament, the Council and the European Economic and Social Committee. Action Plan for an Innovative and Competitive Security Industry," 3.

[41] Ibid., 5.

[42] Ibid.

[43] see for instance Louise Amoore, "Algorithmic War: Everyday Geographies of the War on Terror," *Antipode* 41 (2009); Florian Geyer, "Taking Stock: Databases and Systems of Information Exchange in the Area of Freedom, Security and Justice," *Challenge Research Paper No. 9* (2008); Leese, "Blurring the Dimensions of Privacy? Law Enforcement and Trusted Traveler Programs."; Gary T. Marx and Glenn W. Muschert, "Personal Information, Borders, and the New Surveillance Studies," *Annual Review of Law and Social Science* 3 (2007); Paul de Hert and Rocco Bellanova, *Transatlantic Cooperation on Travelers' Data Processing: From Sorting Countries to Sorting Individuals* (Washington, DC: Migration Policy Institute, 2011).

[44] see for instance Martijn van Otterlo, "A Machine Learning View on Profiling," in *Privacy, Due Process and the Computational Turn. The Philosophy of Law Meets the Philosophy of Technology*, ed. Mireille Hildebrandt and Katja de Vries (Milton Park/New York: Routledge,

security itself has indeed become dominated by the desire to accumulate data in order to predict the future and counter-act criminal and terrorist incidents. But when security is supposed to be enacted through mitigation of future risks, those risks first have to be identified.

ICTs have emerged as the very tools to do so, and such a notion has obviously evoked critical reactions. Thus, ICT research ethics have specifically been concerned with the implications of the use of personal information in distinct contexts.[45] Arguably, the increasing spill-over of ICTs into the realm of security is also the reason why privacy and data protection are framed as predominant ethical concerns of current security research within official EU documents. Whether or not this limitation of ethical concerns to one clear-cut area is by any means adequate remains questionable. It should clearly be noted that multiple other pending ethical issues such as autonomy, social inclusion, human dignity, or dual use and function creep/mission creep between the civil and the military realm of security also do require attention.

However, when looking at the political and financial efforts put into security research over the last decade, one might indeed be under the impression that "our political masters, aided and abetted by the security industry, often appear willing to sacrifice some of the citizenry's privacy in order to better secure society",[46] as van Lieshout et al. have provocatively formulated it. Thus, how come the stark contrast of a presumed trade-off was eventually transformed and is now conceived of as a resolvable privacy by design issue instead of the irreconcilable conflict that it was before?

11.3 A Normative Turn?

The answer arguably lies in the re-framing of the overall European 'security project'. With the Treaty of Lisbon in 2009 and the ensuing legally binding status of the European Charter of Fundamental Rights,[47] the EU has – at least on paper – made a clear commitment to human rights and civil liberties. For the (broader) field of security, this commitment is reflected in the European Internal Security Strategy[48]

2013); Colleen McCue, *Data Mining and Predictive Analysis. Intelligence Gathering and Crime Analysis* (Burlington/Oxford: Elsevier, 2007); Evelien de Pauw et al., eds., *Technology-led Policing* (Antwerpen/Apeldoorn/Portland: Maklu, 2011).

[45] David Wright, "A Framework for the Ethical Impact Assessment of Information Technology," *Ethics and Information Technology* 13 (2011).

[46] van Lieshout et al., "Reconciling Privacy and Security," 120.

[47] European Union. "Charter of Fundamental Rights of the European Union." 2000/C 364/01, 18 December, 2000.

[48] European Union, "Internal Security Strategy for the European Union: Towards a European Security Model."

of 2010 and the Stockholm program that provides the current concrete policy framework (2010–14).[49] The Internal Security Strategy, for instance, explicitly states that "Europe must consolidate a security model, based on the principles and values of the Union: respect for human rights and fundamental freedoms, the rule of law, democracy, dialogue, tolerance, transparency and solidarity."[50] And the Stockholm Programme puts forward a Europe built on human rights, and goes as far as to claim that when it comes to security measures,

> basic principles such as purpose limitation, proportionality, legitimacy of processing, limits on storage time, security and confidentiality as well as respect for the rights of the individual, control by national independent supervisory authorities, and access to effective judicial redress need to be ensured and a comprehensive protection scheme must be established.[51]

This strengthened emphasis on normative aspects of security can also be found in the FP7 security scheme, claiming that "the potential impact of the resulting technologies and activities on Fundamental Rights, ethical principles and societal values should be addressed as part of the proposed research."[52] Again, especially privacy and data protection have thus been officially tagged as norms that potentially become infringed by security technologies.[53] Apart from such official statements, the predominantly technological security tools that have emerged from the FP frameworks in recent years have become the target of normative interventions due to their potential negative impact on society.[54]

Third trajectory. Alongside this new scope on the normative dimension of security, research funding, or rather the governance thereof, is also undergoing change. Security research now has to be 'ethically compliant' in order to take into account possible negative impacts on the societal level. Security research projects are thus to be accompanied by the explicit coverage of ethics boards in order to ensure that research is in line with normative principles. Subsequently, research ethics have come to enact a key role in the governance of security research, and are set to establish safeguards against detrimental societal impacts of security technologies at an early stage during research and development. In EU research

[49] European Council. "The Stockholm Programme – An Open and Secure Europe Serving and Protecting Citizens." Official Journal of the European Union, 2010/C 115/01, 4 May, 2010.

[50] European Union, "Internal Security Strategy for the European Union: Towards a European Security Model," 8.

[51] European Council, "The Stockholm Programme – An Open and Secure Europe Serving and Protecting Citizens," 10.

[52] European Commission. "FP7-SEC-2013-1 Call Fiche, 10 July." 2012, 10.

[53] European Commission. "Ethical and Regulatory Challenges to Science and Research Policy at the Global Level." 2012.

[54] Geyer, "Taking Stock: Databases and Systems of Information Exchange in the Area of Freedom, Security and Justice."; Elspeth Guild and Sergio Carrera, "The European Union's Area of Freedom, Security and Justice Ten Years On," in *The Area of Freedom, Security and Justice Ten Years On: Successes and Future Challenges Under the Stockholm Programme*, ed. Elspeth Guild, Sergio Carrera, and Alejandro Eggenschwiler (Brussels: Centre for European Policy Studies, 2010).

funding, a dedicated ethical coverage of the research process has been introduced as “fundamental ethical principles”[55] since FP5 (1998–2002). Particularly, fields such as medical and biological research have a long history of a need for ethical coverage, as has become apparent by the emerging possibilities of ‘engineering’ human life at the genetic or molecular level. Security research is joining those fields as one of the areas that has be monitored and advised closely. As Burgess notes, “security comes with its own special ethical baggage”,[56] since it carries the potential to inflict curtailments on fundamental societal and individual values. In fact, numerous scholars have in recent years engaged with the threatening and negative consequences of new and emerging security technologies.[57]

However, on the other hand, security itself represents an important value as it “embodies the social and cultural needs of a society, its hopes and fears, its past and its ambitions for the future.”[58] Read through that lens, security represents its own ethics as an overarching prerequisite for any society. Much has been written on the problems that can arise from over-emphasized security and ensuing detrimental impacts on human rights and civil liberties.[59] Adding to that list of potential negative consequences, security research

> can include particular measures that have as a secondary effect an increase in insecurity – such as the development of scanning devices that cause unease, weapons systems that provoke fear or insecurity among innocent bystanders, or surveillance systems that are experienced as too invasive.[60]

Thus, security research appears a Janus-faced phenomenon that possesses the potential of both detrimental and beneficial outcomes that indeed come as “inseparably intertwined.”[61] The delicate balance of the ‘goods’ and ‘bads’ of security for society subsequently underlies constant challenges through security research and the technological tools that emerge from it. A close look reveals, as mentioned earlier, that nearly all security-related research projects within FP7 do feature a technological scope, as “the Security theme supports R&D actions oriented towards

[55] Lisa Stengel and Michael Nagenborg. “Reconstructing European Ethics. How does a Technology Become an Ethical Issue at the Level of the EU? ETICA Deliverable 3.2.2 Annex I.” undated, 2.

[56] Burgess, “Ethical Review and the Value(s) of Security Research,” 2.

[57] see for instance Mark B. Salter, ed. *Politics at the Airport* (Minneapolis/London: University of Minnesota Press, 2008); Didier Bigo and Anastassia Tsoukala, eds., *Terror, Insecurity and Liberty. Illiberal Practices of Liberal Regimes After 9/11* (London/New York: Routledge, 2008); Torin Monahan, ed. *Surveillance and Society. Technological Politics and Power in Everyday Life* (New York/London: Routledge, 2006); David Lyon, ed. *Theorizing Surveillance. The Panopticon and Beyond* (Cullompton/Portland: Willan, 2006); Louise Amoore and Marieke de Goede, eds., *Risk and the War on Terror* (London/New York: Routledge, 2008).

[58] Burgess, “Ethical Review and the Value(s) of Security Research,” 2.

[59] for a comprehensive account, see Jeremy Waldron, “Security and Liberty: The Image of Balance,” *Journal of Political Philosophy* 11 (2003).

[60] J. Peter Burgess. “The Societal Impact of Security Research, PRIO Policy Brief 09/2012.” 2012.

[61] Ibid.

new methodologies and technologies."[62] Due to the sketched potential detrimental impact of security technologies on societies, coupled with the financial volume of security research funding, the stakes for particular security research ethics appear exceptionally high.[63] This constellation is indeed reflected in official documents – and once again it is predominantly framed in terms of privacy. The last call fiche for the security theme of FP7, for instance, states that "if ethical issues, including privacy are raised, they should be addressed in the core of the proposed activity",[64] and the EC document on ethical and regulatory issues in research policy dedicates a whole chapter to "New Security Technologies and Privacy."[65]

This emphasis on privacy arguably comes from the aforementioned data-driven nature of contemporary security technologies that build on the collection and analysis of large amounts of data, as well as from the well-defined legal applicability of the data protection framework that gives privacy concerns a 'procedural advantage' over other normative concerns when it comes to security technologies. The interesting fact is now, that with this 'new' scope on morally right security, the original conflict between security and privacy becomes rather reinforced than mitigated. In other words: with the increased emphasis on the importance of privacy, the privacy side of the original equation has been upgraded and is now not so likely to be overridden by security anymore. And since there no longer seems to be an *a priori* choice which part of the equation should be more cherished, the decisive question then becomes: how to possibly resolve this dilemma and reconcile privacy and security such that their relationship complies with the upgraded normative take on security within the EU? The answer appears indeed an intriguing one: if it is not possible to overcome the conflicting positions of the trade-off (however oversimplified they appear), why not abandon the model, after all? The ensuing move beyond, as enthusiastically announced, has eventually resulted in privacy by design.

11.4 Privacy by Design: A Technological Fix for a Technological Fix?

In the effort to effectively govern emerging technologies from security research, the Commission has identified three main dimensions of regulatory privacy protection: (1) technical, (2) legal, and (3) self-regulatory.[66] Characteristically for the legal dimension is its rather spatial scope, as it is based on the European Convention

[62] http://cordis.europa.eu/fp7/security/about-security_en.html (last accessed 9 January 2014).

[63] Burgess, "Ethical Review and the Value(s) of Security Research."

[64] European Commission, "FP7-SEC-2013-1 Call Fiche, 10 July."

[65] European Commission, "Ethical and Regulatory Challenges to Science and Research Policy at the Global Level," ch. 2.

[66] Ibid., 20.

on Human Rights[67] and the European Charter of Fundamental Rights,[68] rendering its power strongly connected to the jurisdiction of the EU. Within this jurisdiction, legal privacy and data protection provisions possess an enforceable status and thus provides strong incentives for any supplier of security technologies to stay within the explicitly formulated boundaries of data collection and processing. However, in times of global data flows, such a (supra-)national regulation appears hardly up to the task of effective privacy protection.

The self-regulatory dimension of security research governance, on the contrary, is based on voluntary commitments from the private sector. Self-regulation towards technology development that fulfills ethical requirements then is set to be achieved through the involvement of stakeholders and the establishment of 'soft' regulations.[69] The scope within self-regulatory governance lies on non-enforceable concepts such as "market self-regulation, corporate social responsibility (CSR), and governmental incentives for research that can drive technology towards more ethical development."[70] Albeit admitting the potential of voluntary forms of research governance, Székely et al. have pointed out that monitoring and supervision of self-regulation within the area of emerging technologies appears a highly difficult task.[71]

Thus, the official position of the European Commission with regard to security research governance can be summarized such that "weaknesses in self-regulation and legal governance suggest technological governance as a good site for concrete, operationalized engagement with tensions between the protection of privacy and the pursuit of security."[72] One might be inclined to say that this preference in fact appears a technological fix to right the technological fix that is security research in the first place. Now how to achieve such technological reconciliation? From the official documents, it becomes quite clear that Ann Cavoukian's concept of privacy by design[73] is now considered to be the silver bullet for the old clash between

[67] European Court of Human Rights/Council of Europe. "European Convention on Human Rights." 2010.

[68] European Union, "Charter of Fundamental Rights of the European Union."

[69] European Commission, "Ethical and Regulatory Challenges to Science and Research Policy at the Global Level," 20.

[70] Ibid.

[71] Iván Székely, Máté Dániel Szabó, and Beatrix Vissy, "Regulating the Future? Law, Ethics, and Emerging Technologies," *Journal of Information, Communication and Ethics in Society* 9 (2011): 183.

[72] European Commission, "Ethical and Regulatory Challenges to Science and Research Policy at the Global Level," 24.

[73] see for instance Ann Cavoukian. "Privacy by Design. Available at http://www.privacybydesign.ca/content/uploads/2009/01/privacybydesign.pdf (last accessed 26 February 2014)." 2009; Ann Cavoukian, Scott Taylor, and Martin E. Abrams, "Privacy by Design: Essential for Organizational Accountability and Strong Business Practices," *Identity in the Information Society* 3 (2010).

security and privacy. Thus, researchers and developers are encouraged to tackle possible privacy and data protection issues pro-actively from the very beginning in order to avoid costly adjustments later on.

In fact, the ESRIF final report in 2009 made an early effort to bridge the gap between privacy and security and stated that "ESRIF advocates implementation of a 'privacy by design' data protection approach that should be part of an information system's architecture from the start."[74] How does this work? Privacy by design starts with the assumption that "privacy is good for business",[75] and develops the idea that privacy can be conceived of as a positive sum game. This is a crucial notion, as it stands opposed to the postulated zero sum game that is central to the hitherto dominant trade-off model. Furthermore, privacy safeguards then should be implemented proactively and early within the development and design of information processing technologies, and be built in a way that they last throughout the entire product life cycle.

Central in such a conceptualization of the relationship between technology and privacy/data protection is the assumption that privacy principles should be incorporated early in research and development in order to avoid costly retrofits at later stages.[76] It is exactly this presupposition that is now mirrored in EU security research. As stated by the Commission, privacy by design "should be recognized as a guiding and technologically neutral principle, suitable for flexible applications, in a general provision mandating that existing privacy and data protection principles be integrated into ICTs."[77] Just as well, the Action Plan for the security industry suggests to make use of a privacy by design approach.[78] This falls also well in line with recent discussions about privacy-preserving data mining and privacy-enhancing technologies.[79]

But does it really resolve the original conflict, namely the presumable choice between improved security or the protection of privacy? There are a number of issues to be found in the relationship of 'security and/vs privacy' that might not

[74] European Security Research & Innovation Forum, "ESRIF Final Report, available at http://ec.europa.eu/enterprise/policies/security/files/esrif_final_report_en.pdf (last accessed 26 February 2014)," 31.

[75] Cavoukian, Taylor, and Abrams, "Privacy by Design: Essential for Organizational Accountability and Strong Business Practices," 405.

[76] Cavoukian, "Privacy by Design. Available at http://www.privacybydesign.ca/content/uploads/2009/01/privacybydesign.pdf (last accessed 26 February 2014)."

[77] European Commission, "Ethical and Regulatory Challenges to Science and Research Policy at the Global Level," 26.

[78] European Commission, "Communication from the Commission to the European Parliament, the Council and the European Economic and Social Committee. Action Plan for an Innovative and Competitive Security Industry," 11.

[79] Bart Custer et al., eds., *Discrimination and Privacy in the Information Society: Data Mining and Profiling in Large Databases* (Heidelberg/New York/Dordrecht/London: Springer, 2013); Charu C. Aggarwal and Philip S. Yu, eds., *Privacy-Preserving Data Mining: Models and Algorithms* (New York: Springer Science + Business Media, 2008).

be elegantly resolved through privacy by design. A key element in privacy by design are the Fair Information Principles (FIPs), that are set "to limit collection, use and disclosure of personal data, to involve individuals in the data lifecycle, and to apply appropriate safeguards in a continuous manner."[80] Thus, as Schaar argues, this means "the separation of personal identifiers and content data, the use of pseudonyms and the anonymization or deletion of personal data as early as possible."[81] Such practices are undeniably suitable for organizational and economic contexts. However, as has been argued throughout this paper, data-driven security technologies derive their added value exactly from the information surplus that is accumulated through collection and processing of data that could eventually be connected to possible criminals or terrorists in order to cancel out future risks. And we should remember that by the logic of security experts and policy makers, the more information one can get, the better the prediction of the future and thus the better our overall security will be. In other words: security cannot thrive on informational parsimony. FIPs on the contrary radically take away the possibilities that come with advanced analytics in security contexts. This stark contrast stunningly reminds of the early days of security research, when the "trade-off between improved security and loss of privacy"[82] was openly framed as a major obstacle for the field. But how to achieve both effective security and non-intrusive privacy, then?

Certainly, there has been considerable progress in the techniques for data analytics. For instance, algorithms that allow for privacy-preserving ways of data mining[83] have been on the rise in recent years. But even with such privacy-friendly methods of data collection/analytics, the tension between privacy and security cannot be fully resolved. The "dimensionality curse"[84] states that in order to fully preserve privacy, the amount of personal attributes would need to be reduced to such an extent that the utility of processing the data is lost. Hence, the contradicting interests between privacy on the one hand and the benefit of being able to process data on the other hand cannot simply be resolved using technical means. Thus, a certain conflict remains between efficiency in terms of the generation of security knowledge and the preservation of privacy. In simple terms, the more (individual) attributes are reduced from the dataset, the less utility will emerge from analytics. Is

[80] Cavoukian, Taylor, and Abrams, "Privacy by Design: Essential for Organizational Accountability and Strong Business Practices," 406.

[81] Peter Schaar, "Privacy by Design," *Identity in the Information Society* 3 (2010): 267–8.

[82] European Security Research Advisory Board, "Meeting the Challenge: the European Security Research Agenda. A Report from the European Security Research Advisory Board," 8.

[83] Aggarwal and Yu, *Privacy-Preserving Data Mining: Models and Algorithms*.

[84] Charu C. Aggarwal. "On Randomization, Public Information and the Curse of Dimensionality." Paper presented at IEEE 23rd International Conference on Data Engineering, Istanbul, 11–15 April, http://charuaggarwal.net/curse.pdf, 2007; Charu C. Aggarwal and Philip S. Yu. "On Variable Constraints in Privacy Preserving Data Mining." Paper presented at SIAM International Conference on Data Mining, Newport Beach, 21–23 April, http://charuaggarwal.net/aggar140.pdf, 2005.

the turn to privacy by design merely old wine in new bottles, then? Even if it does not convincingly resolve the tension between privacy and security, the transformative framing of the old 'conflict' tells us a lot about the current state of affairs with regard to privacy and security.

11.5 Conclusions

This paper has shown that the relationship between the concepts of privacy and security has come a long way from an early conceptualization as a sharp trade-off towards a contemporary framing as a technological issue that appears resolvable through privacy by design. However, this paper has put forward the claim that the current re-framing is not particularly well suited to actually mitigate or resolve the tension between privacy and security, but rather pays tribute to the technological scope on security, while at the same time acknowledging the increasingly normative take on security with the EU.

The trade-off model has always been troubled by the oversimplified claim that it was possible to put forward two unspecified concepts and outweigh them against each other. And while privacy has long been conceived of as "a moving target",[85] the conceptualization of security is shifting as well. To stay within the metaphor, the second target is also starting to move quite rapidly, as the notion of security is undergoing deep-seated normative transformations. When thinking about the current relationship of privacy and security, it appears only appropriate to take into consideration the changing state of security between abstract concepts, concrete technological applications, economic desires and normative prerequisites and implications.

Is security merely a driver for economic growth and prosperity, or does it indeed come as an intrinsic value that has to be handled with care in order to avoid detrimental effects on societal values? Is privacy a value that is still trumped by the seemingly overarching desire for security, or does it have the capacity to challenge the paradigm of security through the EU's confession to more human rights and civil liberties based security measures and the further incorporation of ethics into EU funded research? The ensuing constellation appears a puzzling one: depending on the perspective, security (technology) is regarded as either a serious threat for privacy or an opportunity for massive economic revenue – but should security by default not be a value itself? A basic need for any society to ensure its present and future prosperity and a safeguard for its individuals to flourish and realize their potential? It remains up for discussion whether privacy by design can provide a true reconciliation of privacy and security, or whether it solely serves as a veil that is set to obscure major concerns with regard to data-driven security technologies. It appears that such a technological approach to the governance of

[85] Friedewald et al., "Privacy, Data Protection and Emerging Sciences and Technologies: Towards a Common Framework," 61.

security research (and subsequently to ‘security’ itself) falls well in line with the general technological scope of EU security research. However, it remains open whether this ‘technological fix for a technological fix’ will strengthen the position of privacy and data protection, or whether security will further trump normative considerations and civil liberties/rights. To end on a critical note: privacy-by-design might not be the silver bullet that it is regarded to be right now, but might rather be a concept that at first sight appears to be easily applicable within the general technological paradigm of security, but only seemingly soothes the conflict between privacy and security.

References

Aggarwal, Charu C. “On Randomization, Public Information and the Curse of Dimensionality.” Paper presented at IEEE 23rd International Conference on Data Engineering, Istanbul, 11–15 April, http://charuaggarwal.net/curse.pdf, 2007.

Aggarwal, Charu C., and Philip S. Yu. “On Variable Constraints in Privacy Preserving Data Mining.” Paper presented at SIAM International Conference on Data Mining, Newport Beach, 21–23 April, http://charuaggarwal.net/aggar140.pdf, 2005.

Aggarwal, Charu C., and Philip S. Yu, eds. *Privacy-Preserving Data Mining: Models and Algorithms*. New York: Springer Science + Business Media, 2008.

Altman, Irwin. “Privacy Regulation: Culturally Universal or Culturally Specific?”. *Journal of Social Issues* 33 (1977): 66–84.

Amoore, Louise. “Algorithmic War: Everyday Geographies of the War on Terror.” *Antipode* 41 (2009): 49–69.

Amoore, Louise, and Marieke de Goede, eds. *Risk and the War on Terror*. London/New York: Routledge, 2008.

Bennett, Colin J. “What Happens When You Book an Airline Ticket? The Collection and Processing of Passenger Data Post-9/11.” In *Global Surveillance and Policing. Borders, Security, Identity*, edited by Elia Zureik and Mark B. Salter, 113–38. Cullompton/Portland: Willan, 2005.

Bigo, Didier, and Julien Jeandesboz. “The EU and the European Security Industry: Questioning the ‘Public-Private Dialogue’. INEX Policy Brief No. 5.” 2010.

Bigo, Didier, and Anastassia Tsoukala, eds. *Terror, Insecurity and Liberty. Illiberal Practices of Liberal Regimes After 9/11*. London/New York: Routledge, 2008.

Burgess, J. Peter. “Ethical Review and the Value(s) of Security Research.” Paper presented at the Workshop Ethical Issues in Security Research – a Practical Approach, Brussels, 29 September, 2011.

Burgess, J. Peter. “The Societal Impact of Security Research, PRIO Policy Brief 09/2012.” 2012.

Cavoukian, Ann. “Privacy by Design. Available at http://www.privacybydesign.ca/content/uploads/2009/01/privacybydesign.pdf (last accessed 26 February 2014).” 2009.

Cavoukian, Ann, Scott Taylor, and Martin E. Abrams. “Privacy by Design: Essential for Organizational Accountability and Strong Business Practices.” *Identity in the Information Society* 3 (2010): 405–13.

Custer, Bart, Toon Calders, Bart Schermer, and Tal Zarsky, eds. *Discrimination and Privacy in the Information Society: Data Mining and Profiling in Large Databases*. Heidelberg/New York/Dordrecht/London: Springer, 2013.

de Hert, Paul, and Rocco Bellanova. *Transatlantic Cooperation on Travelers’ Data Processing: From Sorting Countries to Sorting Individuals*. Washington, DC: Migration Policy Institute, 2011.

de Pauw, Evelien, Paul Ponsaers, Kees van der Vijver, Willy Bruggeman, and Piet Deelman, eds. *Technology-led Policing*. Antwerpen/Apeldoorn/Portland: Maklu, 2011.

ECORYS. "Study on the Competitiveness of the EU Security Industry. Within the Framework Contract for Sectoral Competitiveness Studies – ENTR/06/054: Final Report." 2009.

European Commission. "Commission Staff Working Paper. Impact Assessment. Accompanying the Communication from the Commission 'Horizon 2020 – The Framework Programme for Research and Innovation'." SEC(2011) 1427 final, 30 November, 2011.

European Commission. "Communication from the Commission to the European Parliament, the Council and the European Economic and Social Committee and the Committee of the Regions. Horizon 2020 – The Framework Programme for Research and Innovation." COM(2011) 808 final, 30 November, 2011.

European Commission. "Communication from the Commission to the European Parliament, the Council and the European Economic and Social Committee. Action Plan for an Innovative and Competitive Security Industry." COM(2012) 417 final, 26 July, 2012.

European Commission. "Communication from the Commission. Europe 2020: A strategy for Smart, Sustainable and Inclusive Growth." COM(2010) 2020 final, 3 March, 2010.

European Commission. "Ethical and Regulatory Challenges to Science and Research Policy at the Global Level." 2012.

European Commission. "EU Security Research: Safeguarding Society, Boosting Growth." 2012.

European Commission. "FP7-SEC-2013-1 Call Fiche, 10 July." 2012.

European Commission. "Proposal for a Regulation of the European Parliament and of the Council Laying Down Rules for the Participation and Dissemination in 'Horizon 2020 – the Framework Programme for Research and Innovation (2014–2020)'." COM(2011) 810 final, 30 November, 2011.

European Council. "The Stockholm Programme – An Open and Secure Europe Serving and Protecting Citizens." Official Journal of the European Union, 2010/C 115/01, 4 May, 2010.

European Court of Human Rights/Council of Europe. "European Convention on Human Rights." 2010.

European Security Research & Innovation Forum. "ESRIF Final Report, available at http://ec.europa.eu/enterprise/policies/security/files/esrif_final_report_en.pdf (last accessed 26 February 2014)." 2009.

European Security Research Advisory Board. "Meeting the Challenge: the European Security Research Agenda. A Report from the European Security Research Advisory Board." 2006.

European Security: High Level Study on Threats Responses and Relevant Technologies. "Deliverable D6-1 (Final Report): New European Approaches to Counter Terrorism, 21 March." 2006.

European Union. "Charter of Fundamental Rights of the European Union." 2000/C 364/01, 18 December, 2000.

European Union. "Internal Security Strategy for the European Union: Towards a European Security Model." 2010.

Friedewald, Michael, David Wright, Serge Gutwirth, and Emilio Mordini. "Privacy, Data Protection and Emerging Sciences and Technologies: Towards a Common Framework." *Innovation: The European Journal of Social Science Research* 23 (2010): 61–67.

Geyer, Florian. "Taking Stock: Databases and Systems of Information Exchange in the Area of Freedom, Security and Justice." *Challenge Research Paper No. 9* (2008).

Group of Personalities in the Field of Security Research. "Research for a Secure Europe. Report of the Group of Personalities in the Field of Security Research." 2004.

Guild, Elspeth, and Sergio Carrera. "The European Union's Area of Freedom, Security and Justice Ten Years On." In *The Area of Freedom, Security and Justice Ten Years On: Successes and Future Challenges Under the Stockholm Programme*, edited by Elspeth Guild, Sergio Carrera and Alejandro Eggenschwiler, 1–12. Brussels: Centre for European Policy Studies, 2010.

Hayes, Ben. *Arming Big Brother: The EU's Security Research Programme*. Amsterdam: Transnational Institute/Statewatch, 2006.

Hayes, Ben. *NeoConOpticon. The EU Security-Industrial Complex*. Amsterdam: Transnational Institute/Statewatch, 2009.

Leese, Matthias. “Blurring the Dimensions of Privacy? Law Enforcement and Trusted Traveler Programs.” *Computer Law & Security Review* 29 (2013): 480–90.

Lyon, David. “Airports as Data Filters: Converging Surveillance Systems after September 11th.” *Journal of Information, Communication and Ethics in Society* 1 (2003): 13–20.

Lyon, David, ed. *Theorizing Surveillance. The Panopticon and Beyond.* Cullompton/Portland: Willan, 2006.

Marx, Gary T., and Glenn W. Muschert. “Personal Information, Borders, and the New Surveillance Studies.” *Annual Review of Law and Social Science* 3 (2007): 375–95.

McCue, Colleen. *Data Mining and Predictive Analysis. Intelligence Gathering and Crime Analysis*. Burlington/Oxford: Elsevier, 2007.

Monahan, Torin, ed. *Surveillance and Society. Technological Politics and Power in Everyday Life*. New York/London: Routledge, 2006.

Nissenbaum, Helen. *Privacy in Context: Technology, Policy, and the Integrity of Social Life*. Stanford: Stanford Law Books, 2010.

Regan, Priscilla M. “Response to Bennett: Also in Defence of Privacy.” *Surveillance & Society* 8 (2011): 497–99.

Salter, Mark B., ed. *Politics at the Airport*. Minneapolis/London: University of Minnesota Press, 2008.

Schaar, Peter. “Privacy by Design.” [In English]. *Identity in the Information Society* 3 (2010): 267–74.

Stengel, Lisa, and Michael Nagenborg. “Reconstructing European Ethics. How does a Technology Become an Ethical Issue at the Level of the EU? ETICA Deliverable 3.2.2 Annex I.” undated.

Székely, Iván, Máté Dániel Szabó, and Beatrix Vissy. “Regulating the Future? Law, Ethics, and Emerging Technologies.” *Journal of Information, Communication and Ethics in Society* 9 (2011): 180–94.

Tsoukala, Anastassia. “Risk-focused Security Policies and Human Rights. The Impossible Symbiosis.” In *Mapping Transatlantic Security Relations. The EU, Canada, and the War on Terror*, edited by Mark B. Salter, 41–59. London/New York: Routledge, 2010.

Valkenburg, Govert. “The Trade-Off Model Between Privacy and Security From a Sociotechnical Perspective. Paper presented at Computers, Privacy and Data Protection Conference, Brussels, 22–24 January.” 2014.

van Lieshout, Marc, Michael Friedewald, David Wright, and Serge Gutwirth. “Reconciling Privacy and Security.” *Innovation: The European Journal of Social Science Research* 26 (2013): 119–32.

van Otterlo, Martijn. “A Machine Learning View on Profiling.” In *Privacy, Due Process and the Computational Turn. The Philosophy of Law Meets the Philosophy of Technology*, edited by Mireille Hildebrandt and Katja de Vries, 41–64. Milton Park/New York: Routledge, 2013.

Waldron, Jeremy. “Security and Liberty: The Image of Balance.” *Journal of Political Philosophy* 11 (2003): 191–210.

Warren, Samuel D., and Louis D. Brandeis. “The Right to Privacy.” *Harvard Law Review* 4 (1890): 193–220.

Westin, Alan F. “Social and Political Dimensions of Privacy.” *Journal of Social Issues* 59 (2003): 431–53.

Wright, David. ”A Framework for the Ethical Impact Assessment of Information Technology.” *Ethics and Information Technology* 13 (2011): 199–226.

Part V
Designing and Supporting Privacy and Data Protection

Chapter 12
Evolving FIPPs: *Proactive Approaches to Privacy*, Not Privacy Paternalism

Ann Cavoukian

Abstract Privacy and data protection are at times contrasted with other legitimate societal values and goals, with the suggestion that one must yield to the other. But is it really necessary to weaken existing privacy measures in the name of pursuing greater efficiencies, innovation and economic growth? The goal of reconciling privacy rights with the free flow of data was reaffirmed by the OECD in a multi-year review of the 1980 OECD Guidelines – all eight of the original principles were left intact. This paper examines proposals to abridge these fundamental FIPPs in order to allow for Big Data and other technological and socially beneficial innovations. This paper suggests that the future of privacy depends on informational self-determination as embodied by taking a holistic approach to the FIPPs. Moreover, the paper suggests that the FIPPs be further enhanced through the application of Privacy by Design, which supplements the FIPPs with new elements such as proactively embedding privacy into information technologies, business practices and network infrastructures. Transparency and accountability are also key features in this framework.

12.1 Introduction

Information and communications technologies are transforming our worlds, challenging our ideas of privacy and data protection. Since technological innovations and how we use technology often form the basis of tomorrow's standards, it is natural that important questions be asked regularly about the Fair Information Practice Principles (FIPPs). The enduring tension in these discussions is whether we should create technologies that respect our current understanding of privacy, or whether our understanding of privacy must change in order to allow for new technologies and other developments.

Some privacy professionals, academics and public policy makers believe that the venerable Fair Information Practice Principles (FIPPs) should give way in an

A. Cavoukian (✉)
Information and Privacy Commissioner, Toronto, ON, Canada
e-mail: Michelle.Chibba@ipc.on.ca

S. Gutwirth et al. (eds.), *Reforming European Data Protection Law*,
Law, Governance and Technology Series 20, DOI 10.1007/978-94-017-9385-8_12

era of cloud, social and mobile computing, and the internet of things. They argue that information self-determination is largely a fiction today and that systems of notice and choice, in practice, have become a pointless burden in an era of passive collection of personal information and dense, legalese privacy statements. Purpose specification requirements are out of step with exciting new Big Data applications and insights, prescribing unjustifiable limits on collecting and using personal data, blocking innovation, societal benefits and progress. Better, they argue, to focus on punishing misuses of personal information and to strengthen accountability of data processors/users.[1]

While the intent of these calls may be to shift the burden of privacy protection away from individuals and towards data users/controllers, the effect of such a proposal will be to weaken fundamental privacy rights of individuals, while strengthening the power of data users/controllers to decide what personal data to collect and process, whenever and however they see fit, placing greater burdens on both individuals and regulators to seek effective redress. I consider this a paternalistic approach to privacy.[2]

This paper argues against diminishing the FIPPs – or selectively applying some principles over others – and in support of a proactive approach to privacy that supplements privacy principles in a manner that promotes innovation, privacy, data protection and trust in the twenty-first century.[3] This is consistent with a recent OECD Council recommendation where it noted that, "These Guidelines should be regarded as minimum standards which can be supplemented by additional measures for the protection of privacy and individual liberties, which may impact transborder flows of personal data."[4] The author agrees that accountability should

[1] See specifically Fred H. Cate, Peter Cullen and Viktor Mayer-Schonberger, "Data Protection Principles for the 21st Century, Revising the 1980 OECD Guidelines," December 2013, http://www.oii.ox.ac.uk/publications/Data_Protection_Principles_for_the_21st_Century.pdf ("Cate et al"); See also, Scott Charney, "Microsoft Trustworthy Computing Next" (V1.01), February 2012, http://www.microsoft.com/en-us/download/details.aspx?id=29084; Fred H. Cate and Viktor Mayer-Schonberger, "Notice and Consent in a World of Big Data: Microsoft Global Privacy Summit Summary Report and Outcomes," November 2012, http://www.microsoft.com/en-au/download/details.aspx?id=35596; Craig Mundie, "Privacy Pragmatism," *Foreign Affairs*, February 12, 2014, http://www.foreignaffairs.com/articles/140741/craig-mundie/privacy-pragmatism.

[2] The concept of paternalism refers to: "The attitude or actions of a person, or organization, that protects people and gives them what they need, but does not give them any responsibility or freedom of choice." *Merriam-Webster Online Dictionary*, s.v. "paternalism," http://www.merriam-webster.com/dictionary/paternalism. See also Daniel Solove, "Privacy Self-Management and the Consent Dilemma." *Harvard Law Review*. 126 (2013): 1879–2139.

[3] Office of the Information and Privacy Commissioner of Ontario, "Landmark Resolution Passed to Preserve the Future of Privacy," October 29, 2010, http://www.ipc.on.ca/images/Resources/2010-10-29-Resolution-e_1.pdf.

[4] OECD, "Recommendation of the Council concerning Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data (2013)," at 6, http://acts.oecd.org/Instruments/ShowInstrumentView.aspx?InstrumentID=114&InstrumentPID=312&Lang=en&Book=False ("OECD Privacy Framework").

be strengthened, and there are many ways to achieve this using a proactive approach to privacy rather than diminishing the FIPPs.[5]

It is clear the world is changing. The expectation placed on individuals to navigate through dense and lengthy privacy notices and policies to protect their privacy is unsustainable. However, as stated by the Article 29 Working Party of the European Commission (WP29), in their opinion on purpose limitation, "[w]hen we share personal data with others, we usually have an expectation about the purposes for which the data will be used."[6] Big Data analytics, the Internet of Things, and Cloud Computing are all trends that may yield remarkable new correlations, insights, and benefits for society at large. While there is no intention that privacy should stand in the way of progress, it is essential that privacy practitioners participate in these efforts to shape trends in a way that is truly constructive, enabling both privacy and these technology advances to develop, in tandem.[7] As a privacy community, we must explore the question of how to reconcile, on the one hand, the practical challenges of implementing FIPPs in new technological environments with, on the other hand, the individual's expectation of privacy. However, we will have already failed in our endeavours if we begin these discussions by adopting a zero-sum perspective.

12.2 Privacy Paternalism: Removing Limits and Obligations Related to the Collection Principle

Removing obligations to obtain informed consent when collecting personal information could have sweeping impacts on the privacy of individuals. In many contexts, providing effective "notice and choice" to individuals about data

[5] Ann Cavoukian, "Identity Theft Revisited: Security Is Not Enough," September 2005, http://www.ipc.on.ca/images/Resources/idtheft-revisit.pdf; Ann Cavoukian, Martin E. Abrams, and Scott Taylor, "Privacy by Design: Essential for Organizational Accountability and Strong Business Practices," November 2009, http://www.ipc.on.ca/images/Resources/pbd-accountability_HP_CIPL.pdf; Ann Cavoukian and Terry McQuay, "A Pragmatic Approach to Privacy Risk Optimization: Privacy by Design for Business Practices," November 2009, http://www.ipc.on.ca/images/Resources/pbd-privacy-risk.pdf; Ann Cavoukian, "Privacy Risk Management: Building Privacy Protection into a Risk Management Framework to Ensure that Privacy Risks Are Managed, By Default," April 2010, http://www.ipc.on.ca/images/Resources/pbd-priv-risk-mgmt.pdf.

[6] Article 29 Data Protection Working Party, "Opinion 03/2013 on purpose limitation," April 2, 2013, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf, p. 4. ("Opinion 03/2013")

[7] For a brief discussion, see Eduardo Ustarian, "The Privacy Pro's Guide to the Internet of Things," *IAPP Dashboard*, February 12, 2014, http://bit.ly/1lTEo5c.

processing operations may seem like an unnecessary, pointless burden.[8,9] Notices can be long and complicated, hard to understand and inconvenient for individuals; and practical options may be limited. In the emerging Big Data, the Internet of Things, and Cloud Computing environments, the individual is often unaware of data collection taking place or is completely absent from the transaction and processing.[10] Nevertheless, the problems with "notice and choice" should not be used as a simple justification for diminishing consent.

Despite the difficulties with the concept,[11] and despite their being other legitimate bases for the collection of personal information,[12] informed consent – explicit or implicit – remains the cornerstone of modern FIPPs[13] and is foundational to modern private sector privacy laws in force around the world. Diminishing the central role of consent diminishes the individual's right and ability to participate in the management of their personal data by others, undermining the application of other FIPPs which are complementary and intended to be applied holistically.[14]

[8] The final FTC Consumer Privacy Report (2012) and the E.U. Article 29 Working Party Opinion 15/2011 discuss the challenges of obtaining consent in more detail. Federal Trade Commission, "Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers," March 2012, http://www.ftc.gov/reports/protecting-consumer-privacy-era-rapid-change-recommendations-businesses-policymakers; Article 29 Data Protection Working Party, "Opinion 15/2011 on the definition of consent," http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp187_en.pdf.

[9] It is important to note that the term "notice and choice" refers to the system of obtaining consent specifically in the U.S., which does not have overarching FIPPs-based privacy legislation found in Europe and Canada. Marc Rotenberg, "Fair Information Practices and the Architecture of Privacy (What Larry Doesn't Get)," *Stanford Technology Law Review*, 1 (2001): 1–4.

[10] Ann Cavoukian, "Privacy in the Clouds," May 2008, http://bit.ly/1ka4eQ6.

[11] Criticisms include that consent legitimizes any collection, is often collected in a take it or leave it manner, does not offer a way to control downstream uses of data, and does not offer explicitly the right to delete consent. OECD, "Privacy Expert Group Report on the Review of the 1980 OECD Privacy Guidelines", OECD Digital Economy Papers, No. 229, OECD Publishing (2013) ("OECD Privacy Expert Report") http://dx.doi.org/10.1787/5k3xz5zmj2mx-en; Bart Custers, Simone van der Hof et al. (2013). "Informed Consent in Social Media Use: The Gap between User Expectation and EU Personal Data Protection Law." Scripted 10 (4).

[12] COM (2012) 11/4 Draft 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), Article 6.

[13] See, for example, ISO/IEC, *ISO/IEC 29100:2011 Information Technology – Security Techniques – Privacy Framework.*

[14] Ibid, *OECD Privacy Framework*, paragraph 7. "As an introductory comment on the principles set out in Paragraphs 7 to 14 of the Guidelines it should be pointed out that these principles are interrelated and partly overlapping. Thus, the distinctions between different activities and stages involved in the processing of data which are assumed in the principles, are somewhat artificial and it is essential that the principles are treated together and studied as a whole. The principles in these Guidelines are complementary and should be read as a whole."

Consent is multi-dimensional. It is so much more than permission to a one-time collection of personal information. Lacking the opportunity to provide informed consent, the individual is effectively disempowered. Consent empowers individuals to exercise additional privacy rights and freedoms, such as the ability to:

- make consent conditional;
- revoke consent;
- deny consent for new purposes and uses;
- be advised of the existence of personal data record-keeping systems;
- access personal data held by others;
- verify the accuracy and completeness of one's personal data;
- obtain explanation(s) of the uses and disclosures of one's personal data; and
- challenge the compliance of data users/controllers.

Informed and empowered individuals serve as essential checks on the uses and misuses of personal data, holding data processors accountable in a way no law, regulation or oversight authority could ever do. In Germany, the concept of informational self-determination was created over 30 years ago by the Constitutional Court who derived it from their Constitution in 1983.[15] This captures the central role that the individual is expected to play in determining the uses of his or her personal data. Individuals are intended to feature prominently in considering the acceptable secondary uses of their personal data. Central to this determination is context – context is key to determining what may be considered an appropriate secondary use, and is often lacking without the involvement of the data subject.

Removing consent from the data collection equation risks undermining fundamental individual rights, protections and freedoms far beyond "notice and choice" systems. Instead of doing away with consent, we should work at strengthening, not weakening consent by improving transparency and individual control mechanisms – addressing the challenges head-on.

Another criticism of consent which focuses on the practicality of providing notice, should not close out the possibility of moving beyond our current system of notices, and beyond existing enhancements (e.g. tables, icons, and layers), towards the possibility of a new generation of notices, such as notices based on experiences of technology (i.e. 'visceral notice').[16]

In sum, many would agree that there is poor understanding of individual responses to notice and choice options, and until they are resolved, they should not be used as a proposition for arguments to remove or limit obligations under the collection principle.

[15] Gerrit Hornung, and Christoph Schnabel. (2009). *Computer Law & Security Report* (Vol. 25), pg. 84–88, http://dx.doi.org/10.1016/j.clsr.2008.11.002.

[16] Ryan Calo, "Against Notice Skepticism in Privacy (and Elsewhere)," *Notre Dame Law Review* 87:3 (2012): 1027–72.

12.3 Why Eliminate Purpose Specification?

Another foundational FIPPs is Purpose Specification: “The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfilment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.”[17] Purposes are the basis for setting and evaluating limits on collection and use of personal information, and for determining necessity and proportionality.

Some argue that with a diminished need to notify data subjects and obtain their consent, there should be less duty to specify purposes in advance. They argue that some purposes are implied or do not require consent, such as fulfilling an order, improving service quality or cooperating with law enforcement authorities. Others argues that it is impossible to know in advance all of the possible uses and benefits of personal information, and that specifying or limiting purposes unnecessarily limits those future uses and benefits. Non-existent or excessively broad purposes permits a wide spectrum of compatible uses and allows indefinite data retention “just in case.”

The central problem here is that eliminating purpose limitation gives an unprecedented free hand to data users/controllers – public or private, large or small, wherever in the world they may be located, to unilaterally decide why, what, or when personal data should be collected, used and disclosed, with little input from data subjects or oversight authorities.

Lacking sufficient restraints and taking a paternalistic approach could lead to what privacy advocates fear most – ubiquitous mass surveillance, facilitated by more extensive, and detailed profiling, sharpened information asymmetries and power imbalances, ultimately leading to various forms of discrimination.[18] A greater burden would be placed upon both individuals and regulators to prove harms, establish causation, and seek effective redress – the exact opposite of taking a proactive approach to privacy which emphasizes prevention and the taking of proactive measures.[19]

If the history of privacy has taught us anything, it is that an individual’s loss of control over their personal data leads to more and greater privacy abuses, not fewer and smaller. It is not difficult to imagine how this proposal to eliminate purpose specification, if implemented, could lead to a “collect the entire haystack” mentality, and to overbroad or unspecified and undesirable secondary uses – “fishing expedition” methods of data processing. When making decisions affecting individuals, out-of-date or incomplete data, incorrect inferences, and automated decision-making processes can have profoundly negative consequences.

[17] “Purpose Specification,” OECD Privacy Principles, http://oecdprivacy.org/#purpose.

[18] Ibid, Opinion 03/2013, p. 45–46. See also discussion in Omer Tene & Jules Polonetsky, “Big Data for All: Privacy and User Control in the Age of Analytics,” *New Jersey Journal of Technology and Intellectual Property*, 239:11 (2013).

[19] Ann Cavoukian, “Privacy by Design: Leadership, Methods, and Results,” in *European Data Protection: Coming of Age*, ed. S. Gutwirth et al. (New York: Springer, 2013), 175 (“Leadership”).

The Purpose Specification principle is even more critical when individual participation and consent have been diminished. Whether or not consent is informed or explicit, individuals will always have basic expectations about how their personal data is to be used, namely, that it will be used for the purpose(s) for which they provided it. There is a natural expectation that there will be some basic limitations when an individual provides his/her personal data. The individual does not hand over his/her information to the government or a business to do with it whatever it wants.

On April 2, 2013, the WP29 provided an opinion on the principle of purpose limitation. In particular, the WP29 discussed the principle of purpose limitation under the current European Union ("EU") Directive 95/46/EC and provided recommendations for the proposed EU General Data Protection Regulation.

In the WP29 Opinion, the WP29 stated that purpose limitation protects individuals by restricting how data controllers use personal information, while also providing a degree of flexibility. The WP29 further described purpose limitation as being comprised of two elements: (1) purpose specification; and (2) compatible use. The WP29 explained the relationship between these two elements by referencing Article 6(1)(b) of the EU Directive which states that personal information must only be collected for "specified, explicit and legitimate purposes" (purpose specification) and not be "further processed in a way incompatible" with those purposes (compatible use).[20]

The WP29 also stated the following: "The prohibition of 'incompatibility' in Article 6(1)(b) does not altogether rule out new, different uses of the data – provided that this takes place within the parameters of compatibility."[21] The WP29 goes on to state that compatibility needs to be assessed on a case-by-case basis, with the following factors taken into account:

- the relationship between the purposes for which the personal data have been collected and the purposes of further processing;
- the context in which the personal data have been collected and the reasonable expectations of the data subjects as to their further use;
- the nature of the personal data and the impact of the further processing on the data subjects;
- the safeguards adopted by the controller to ensure fair processing and to prevent any undue impact on the data subjects.[22]

Similarly, from a public sector viewpoint, in the jurisdiction of Ontario, Canada, the *Freedom of Information and Protection of Privacy Act* (*FIPPA*) and its municipal equivalent (*MFIPPA*) limit an institution's ability to use information in its custody and control.[23]

[20] Ibid, Opinion 03/2013, p. 3.

[21] Ibid, p. 4.

[22] Ibid, p. 3.

[23] Specifically, section 41(1)(b) of *FIPPA* and section 31(b) of *MFIPPA* state that: "An institution shall not use personal information in its custody or under its control except, (b) for the purpose for

In determining whether the individual might reasonably have expected such a use or disclosure, the practice of the Information and Privacy Commissioner of Ontario has been to impose a “reasonable person” test. Therefore, the question that must be asked is whether an individual would have reasonably expected the use of their personal information for the identified purposes. Investigation reports issued by the Commissioner have found that there must be a rational connection between the purpose of the collection and the purpose of the use, in order to meet the “reasonable person” test. In applying the “reasonable person” test and determining whether there is a rational connection, the Commissioner considers many factors, including the factors listed by the WP29 when assessing compatibility.

It is important to note that section 43 of *FIPPA* and section 33 of *MFIPPA* define “consistent” purpose in relation to personal information that has been collected *directly* from the individual. Where information has been collected *indirectly*, a consistent purpose would be one that is “reasonably compatible” with the purpose for which the personal information had been obtained. Note that Ontario’s “reasonably compatible” language is virtually identical to the E.U. WP29 “compatible use” language. The Commissioner’s practice when assessing “reasonably compatible” purposes is not an “identical purpose” test; rather, the Commissioner will look to what the wording and intent of the indirect collection of the information indicates.

It should also be noted that when a consistent purpose cannot be established, Ontario institutions may still use the personal information in their custody or control if the person to whom the information relates has identified that information and consented to its use.[24]

As evidenced above, privacy legislation in both the EU and Ontario, Canada, place justifiable limits and provide flexibility on a data user/controller’s collection, use and disclosure of personal information.

12.4 Concerns with a New Use Principle of Balancing Benefits with Harms to Individuals

The call to substantially revise the Use Limitation principle[25] to introduce the notion that the data user/controller should balance benefits of the use, with harms to the individual and harm mitigation tools in place for each intended data use, is of great

which it was obtained or compiled or for a consistent purpose.” In determining whether a use is “consistent” with the primary purpose, section 43 of *FIPPA* and section 33 of *MFIPPA* provide that a use or disclosure will be considered consistent only if “the individual might reasonably have expected such a use or disclosure.”

[24] Section 41(1)(a) of *FIPPA*. Please note that section 41(1) of *FIPPA* and 31 of *MFIPPA* specify other purposes for which an institution may use personal information, most of which are beyond the scope of this paper.

[25] Ibid, Cate et al. p. 15–16.

concern. This approach would lead to a "race to the bottom" scenario. In this new Use Principle, there is the concept that harms to the individual "should be permitted with protections." By what standards should benefits and harm be evaluated – to the individual, society, or a company's bottom line? It is difficult to support any principle that would allow foreseeable harms to individuals even if safeguards are employed. In addition, such safeguards are chosen not by the individual, but by the data user/controller, and may or may not include the "protection" of consent.

Even if a harms-based approach to privacy was feasible, we are a long way from achieving meaningful national, let alone international, consensus on defining "harms" (nor broadening the scope). We are far from … "put[ting] in place practical frameworks and processes for identifying, balancing, and mitigating those harms."[26] And who would do this? U.S. courts have been reluctant to step in on behalf of affected individuals.[27]

Absent clearly defined and agreed standards for privacy-related "harms," any call to liberalize the market for using personal data should be viewed with skepticism. As noted above, individuals would be significantly disadvantaged by the lack of notice and consent, and the minimization of their ability to participate in the process. Any significant loss of individual autonomy in relation to one's personal data should be viewed as harmful.

Greater accountability for the uses of personal data is critical.[28] However, the call to diminish the Use Limitation principle shifts the burden of proof to demonstrate the existence of harm to individuals, with regulators officiating such cases to document the harms, to prove causality, and then seek redress. Proving the causality of harms is notoriously difficult to do, and will likely become even more so in the current era of complex, interconnected global information systems and networks that are increasingly opaque to both individuals and oversight authorities.

Even today, harms arising from cases of identity theft due to a security breach are difficult to prove. Similarly, establishing links between poor organizational data-handling practices and the negative effects of individuals being erroneously placed on a watchlist or other similar blacklist, losing an employment opportunity, paying a higher insurance premium, being denied health coverage, or suffering a damaged reputation or the inability to travel, can be a Kafkaesque experience.

While superficially appealing in theory, in practice, harms tests are far too narrow a basis for effectively protecting privacy in this day and age.[29] As the name

[26] Ibid.

[27] See Dana Post, "Plaintiffs Alleging Only 'Future Harm' Following a Data Breach Continue to Face a High Bar," *IAPP Privacy Advisor*, January 29, 2014, http://bit.ly/1qj1ilS.

[28] Indeed, important work has been carried out in this area in recent years by the OECD, the E.U. Commission, the FTC in the United States, and many other public and private sector industry associations, standards-setting bodies and advocacy groups.

[29] See discussion by Ryan Calo, "The Boundaries of Privacy Harm," *Indiana Law Journal* 86:3 (2011). See also "FTC, Exploring Privacy – A Roundtable Series," 1st Roundtable Series, Remarks of Marc Rotenberg, Electronic Privacy Information Center, at 301; 1st Roundtable, Remarks of Leslie Harris, Center for Democracy & Technology, at 36–38; 1st Roundtable, Remarks of

implies, harms tests are fundamentally reactive, allowing harms to arise rather than proactively preventing the harm, right from the outset. The effect of such a proposal will be to retard the development and application of real, effective preventative remedies.[30] In the meantime, a mountain of unnecessary harms will have occurred, responsibility for which will most likely go undetected and unchallenged. A flexible, robust set of FIPPs, ideally embedded into design, remains the best bulwark against future harms (material or immaterial). There should be greater emphasis on preventative methods, such as conducting comprehensive privacy impact assessments (PIAs). Moreover, regulators' resources are already stretched to the limit, and it is highly unlikely that additional staffing will be provided to absorb the additional burdens imposed by such a proposal. The opposite is happening – resources are shrinking, not expanding.

12.5 Privacy Does Not Stand in the Way of Innovation

Some suggest that rigid adherence to general privacy principles inhibits innovation and interferences with economic and social progress, and that these limits should be relaxed. We should be wary of good intentions and seek ways to achieve positive-sum outcomes. Many of the perceived barriers associated with obtaining informed consent, specifying and limiting purposes, and restricting collection and uses of personal information can be obviated by applying innovative methods and widely available data processing techniques. Many Big Data applications may be achieved using de-identified data in place of identifiable personal information. For example, Dr. Khaled El Emam, Professor at the University of Ottawa and Canada Research Chair in Electronic Health Information, has developed a tool that de-identifies personal information in a manner that simultaneously minimizes both the risk of re-identification and the degree of distortion to the original database.[31] The European Data Protection Commissioners have developed criteria and practical guidelines on open data and public sector information re-use,[32] as has the Office of the Information and Privacy Commissioner of Ontario, Canada.[33]

Susan Grant, Consumer Federation of America, at 38–39: http://www.ftc.gov/bcp/workshops/privacyroundtables/index.shtml

[30] Stuart Shapiro, "The Risk of the 'Risk-Based Approach'" *The IAPP Daily Dashboard*, March 31, 2014, http://bit.ly/1hBUokp.

[31] Khaled El Emam. *Guide to the De-Identification of Personal Health Information* (CRC Press, 2013); Khaled El Emam, and Luk Arbuckle. *Anonymizing Health Data: Case Studies and Methods to Get You Started* (O'Reilly Media, Inc., 2013).

[32] Article 29 Data Protection Working Party, "Opinion 06/2013 on Open Data and Public Sector Information ('PSI') Reuse."

[33] Ann Cavoukian, "Access by Design: The 7 Fundamental Principles," April 2010, http://bit.ly/1hhJKUQ.

Privacy and data protection are at times contrasted with other legitimate societal values and goals, with the suggestion that one area must yield to the other. It is not necessary to weaken existing privacy measures in the name of pursuing greater efficiencies, innovation and economic growth. Further, there is a long and growing list of public and private-sector authorities in the United States, the EU, and elsewhere, who unequivocally endorse a proactive approach to privacy as a more robust application of FIPPs, and as a critical means by which to establish sufficient, necessary *trust* in the evolving information economy.[34]

12.6 Evolving Privacy Through Proactive Approaches to Privacy

In contrast to those who would reduce or remove existing FIPPs, others argue that the current principles must be supplemented with additional protections. Some say the current model should not be abandoned, but since technically legal uses of personal information can still be unfair "further discussion on other, additional models" would be useful.[35] It is the argument of this paper that the proactive approaches to privacy should be adopted as one of these additional models.

For example, *Privacy by Design* Foundational Principles build upon universal 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 privacy and security by:

- serving as a framework for domain-specific control objectives and best practices;
- reducing harms and other "unintended" consequences associated with personal information;
- strengthening internal accountability mechanisms;
- demonstrating effectiveness and credibility of data management practices;
- supporting regulatory and third party oversight efforts;
- earning the confidence and trust of clients, partners and the public; and
- promoting market-based innovation, creativity and competitiveness.

[34] These include, *inter alia*, the U.S. White House, Federal Trade Commission, Department of Homeland Security, Government Accountability Office, European Commission, European Parliament and the Article 29 Working Party, among other public bodies around the world who have passed new privacy laws based upon the FIPPs. In addition, international privacy and data protection authorities unanimously endorsed *Privacy by Design* as an international standard for privacy.

[35] Ibid, Custers et al; Paula Bruening, "Data Privacy Day 2014," January 28, 2014, Intel Corporation, http://blogs.intel.com/policy/2014/01/28/today-day-rethink-privacy.

The 7 Foundational Principles of *Privacy by Design* are summarized as follows[36]:

- Use proactive rather than reactive measures, anticipate and prevent privacy invasive events *before* they happen (*Proactive* not Reactive; *Preventative* not Remedial)
- Personal data must be automatically protected in any given IT system or business practice. If an individual does nothing, their privacy still remains intact (Privacy as the *Default*)
- Privacy must be embedded into the design and architecture of IT systems and business practices. It is not bolted on as an add-on, after the fact. Privacy is integral to the system, without diminishing functionality (Privacy *Embedded* into Design)
- All legitimate interests and objectives are accommodated in a positive-sum manner (Full Functionality – *Positive-Sum*, not Zero-Sum)
- Security is applied throughout the entire lifecycle of the data involved – data are securely retained, and then securely destroyed at the end of the process, in a timely fashion (End-to-End Security – *Full Lifecycle Protection*)
- All stakeholders are assured that whatever the business practice or technology involved, it is in fact, operating according to the stated promises and objectives, subject to independent verification (*Visibility* and *Transparency* – Keep it *Open*)
- Architects and operators must keep the interests of the individual uppermost by offering such measures as strong privacy defaults, appropriate notice, and empowering user-friendly options (*Respect* for User Privacy – Keep it *User-Centric*)

There are many public- and private-sector authorities in the United States, the European Union, and elsewhere, who endorse proactive approaches to privacy. They do so acknowledging *PbD* as a more robust application of the FIPPs in establishing and ensuring trust in the evolving information economy.[37] *Privacy by Design* builds upon FIPPs by emphasizing proactive leadership and goal-setting, systematic and verifiable implementation methods, and demonstrable positive-sum results by dealing with privacy issues early on, embedding privacy into the design of systems, and ensuring the full functionality of systems is not sacrificed for privacy.

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. When embedding privacy and data protection into a given information technology, process, system, or architecture, it can be done in

[36] Ann Cavoukian, “The 7 Foundational Principles of Privacy by Design,” January 2009, http://bit.ly/1gcDTMd.

[37] These include, *inter alia*, the U.S. White House, Federal Trade Commission, Department of Homeland Security, Government Accountability Office, European Commission, European Parliament and the Article 29 Working Party, among other public bodies around the world who have passed new privacy laws based upon the FIPPs. In addition, international privacy and data protection authorities unanimously endorsed *Privacy by Design* as an international standard for privacy.

such a way that full functionality is not impaired, and that all legitimate interests are accommodated and requirements optimized.[38]

As noted above, a revised set of OECD guidelines was published in July 2013, based on a comprehensive review by The Privacy Experts Group of the OECD Working Party on Information Security and Privacy. Indeed, the OECD members had already identified a number of elements believed to be critical to improving the effectiveness of privacy protections that included, for example, "embedding privacy by design into privacy management processes."[39]

12.6.1 Innovate by Focussing on the Individual

The prevailing "Notice and Choice" model has many flaws and needs to be strengthened towards a more robust individual "Transparency and Control" model. Proactive approaches to privacy are inherently user-centric,[40] which encourages innovation in this area, for example, by furthering the "SmartData" concept,[41] which automatically restricts secondary uses within user-centric devices. Trusted online agents and third parties would minimize the creation and processing of personal data automatically, acting as intermediaries and enforcers of individual privacy preferences. Such systems, promise to extend the ability of individuals to exercise meaningful control over their personal data.

It is readily acknowledged that there is much room for innovation to address the needs of an evolving world where individuals are acting less and less as direct parties to online transactions; as such, they have less opportunity to exercise meaningful participation in the lifecycle of their personal data.[42] Considerable work on user-centric, privacy-enhancing and transparency-enhancing technologies is being undertaken by leading EU and US researchers,[43] and is deserving of greater

[38] For examples of positive sum see Ibid, Cavoukian, "Leadership," p. 190.

[39] Ibid, OECD, Paper No. 229.

[40] "User" here refers to the data subject.

[41] See generally IPSI Smart Data International Symposium, http://www.ipsi.utoronto.ca/sdis/.

[42] Ibid, Cavoukian, "Privacy in the Clouds."

[43] See, for example, Carnegie-Mellon University CyLab Usable Privacy and Security Laboratory (CUPS), http://cups.cs.cmu.edu, "Future of Identity in the Information Society (FIDIS)," http://www.fidis.net, "Privacy and Identity Management for Europe (Prime)," http://www.prime-project.eu, "Trustworthy Clouds Privacy and Resilience for Internet-Scale Critical Infrastructure (TClouds)," http://www.tclouds-project.eu, "Privacy and Identity Management for Community Services (PICOS)," http://www.picos-project.eu, Ann Cavoukian & Drummond Reed, "Big Privacy: Bridging Big Data and the Personal Data Ecosystem through Privacy by Design," December 2013, http://www.ipc.on.ca/english/Resources/Discussion-Papers/Discussion-Papers-Summary/?id=1352, Ibid, Cavoukian. "Privacy in the Clouds," Ann Cavoukian & Justin Weiss, "Privacy by Design and User Interfaces: Emerging Design Criteria – Keep It

attention and support. As pointed out by Neelie Kroes, European Commission Vice-President: "Privacy is not just about technical features. Without privacy, consumers will not trust the online world. And without trust, the digital economy cannot reach its full potential."[44]

In addition, the Personal Data Ecosystem (PDE) is an emerging trend supported by a number of companies and organizations[45] that have developed tools and technologies to enable the individual to have much greater management and control over his/her personal information than is currently possible today.[46] Another concept is Personal Data Management (PDM) or monetisation[47] of one's data achieved through various types of architectures, where the bottom line is that an individual's data is not shared without his/her consent, or in the case of necessity, on condition that the data will not be used for other purposes than originally identified.[48]

A proactive approach to privacy places the onus upon data users/controllers to anticipate and acknowledge the individual's right to control wherever possible. An essential principle should be that data users/controllers should engineer information technologies, organizational processes and networked systems with the most privacy-protective default settings. This is essentially an opt-in model involving the individual's positive consent for additional secondary uses of their data.

12.7 Conclusion

There is a growing understanding that innovation and competitiveness must be approached from a "design-thinking" perspective – namely, viewing the world to overcome constraints in a way that is holistic, interdisciplinary, integrative, creative and innovative. The future of privacy must also be approached from the same design-thinking perspective. Privacy and data protection should be incorporated into networked data systems and technologies by default, and become integral to organizational priorities, project objectives, design processes, and planning

User-Centric," June 2012, http://ww.ipc.on.ca/English/Resources/Discussion-Papers/Discussion-Papers-Summary/?id = 1201.

[44] Neelie Kroes, "Online privacy – reinforcing trust and confidence," (speech, Brussels, June 22, 2011), European Union, http://europa.eu/rapid/press-release_SPEECH-11-461_en.htm.

[45] See, for example, the list of member companies at Personal Data Ecosystem Consortium, http://pde.cc/startup-circle.

[46] Ann Cavoukian, "Personal Data Ecosystem (PDE) – A Privacy by Design Approach to an Individual's Pursuit of Radical Control," in *Digital Enlightenment Forum Yearbook 2013: The Value of Personal Data*. M. Hilldebrandt, K. O'Hara and M. Waidner (eds). IOS Press. ("PDE").

[47] "Monetize": "to utilize (something of value) as a source of profit," *Merriam Webster Online,* http://www.merriam-webster.com/dictionary/monetize.

[48] Ibid, Cavoukian, "PDE."

operations. Ideally, privacy and data protection should be embedded into every standard, protocol, and data practice that touches our lives. This will require skilled privacy engineers, computer scientists, software designers and common methodologies that are now being developed, hopefully to usher in an era of Big Privacy.

This paper outlines that we must be careful not to naively trust data users/controllers, or unnecessarily expose individuals to new harms, unintended consequences, power imbalances and data paternalism. A "trust me" model will simply not suffice. In light of Edward Snowden's revelations of widespread mass surveillance by the state, with governments also gaining access to large databases in the private sector (as well as the historical record of state abuses), one has to question the desirability of lowering the standards of privacy and data protection.

Those who would argue that privacy principles prevent much-needed and altruistic uses of data, in order to advance societal interests must understand that the indiscriminate collection of personally identifiable data could cause irreparable harm to individuals, and such practices may also impede much sought-after progress in the sciences, health sector, and education. For example, in the case of Big Data, one may argue for the need to "gather the haystack" in order to "find the needle," when in reality, it could be much easier to find the needle without the haystack. Indeed, as noted by Alexander Dix, Commissioner for Data Protection and Freedom of Information Berlin, Germany in a recent webinar Big Data Calls for Big Privacy – Not Only Big Promises, "there is no viable (acceptable) business model for Big Data applications which neglects the individual's right to informational autonomy. The possible benefits of Big Data can be achieved by intelligently taking privacy into account."[49]

The default cannot be "collect all the data" in personally identifiable form. Privacy should be the default setting. But within that context, great strides may be made in data science and Big Data analytics. This is not an either/or proposition – abandon zero-sum thinking.

As the basis of privacy legislation around the world, FIPPs should remain inherently intact and may be further enhanced through the application of *Privacy by Design*, which adds new elements to traditional FIPPs, such as proactively embedding privacy into information technologies, business practices, and network infrastructures. By doing so, individuals are not placed in the position of having to be concerned about safeguarding their personal information – they can be confident that privacy is assured, right from the outset.

[49] Information and Privacy Commissioner of Ontario (Producer). January 24, 2014. "Big Data Calls for Big Privacy – Not Big Promises" [Video webcast]. Retrieved from http://www.privacybydesign.ca/index.php/webinar-big-data-calls-big-privacy-big-promises/.

Bibliography

Carnegie-Mellon University CyLab Usable Privacy and Security Laboratory (CUPS), http://cups.cs.cmu.edu.

“Exploring Privacy – A Roundtable Series,” http://www.ftc.gov/bcp/workshops/privacyroundtables/index.shtml.

“Future of Identity in the Information Society (FIDIS),” www.fidis.net.

“IPSI Smart Data International Symposium,” http://www.ipsi.utoronto.ca/sdis/.

“Personal Data Ecosystem Consortium,” http://pde.cc/startup-circle.

“Privacy and Identity Management for Community Services (PICOS),” www.picos-project.eu.

“Privacy and Identity Management for Europe (PRIME),” www.prime-project.eu.

“OECD Privacy Principles,” http://oecdprivacy.org.

“Trustworthy Clouds Privacy and Resilience for Internet-Scale Critical Infrastructure (TClouds)”, www.tclouds-project.eu.

Ann Cavoukian, “Identity Theft Revisited: Security Is Not Enough”, Office of the Information & Privacy Commissioner of Ontario http://www.ipc.on.ca/images/Resources/idtheft-revisit.pdf.

Ann Cavoukian, “Personal Data Ecosystem (PDE) – A Privacy by Design Approach to an Individual’s Pursuit of Radical Control,” in *Digital Enlightenment Forum Yearbook 2013: The Value of Personal Data*. M. Hilldebrandt, K. O’Hara and M. Waidner (eds). IOS Press, 2013.

Ann Cavoukian, “Privacy by Design: Leadership, Methods, and Results,” in European Data Protection: Coming of Age, ed. S. Gutwirth et al. (New York: Springer, 2013), 175.

Ann Cavoukian, *Privacy in the Clouds: Privacy and Digital Identity – Implications for the Internet* 2008 http://www.ipc.on.ca/images/Resources/privacyintheclouds.pdf.

Ann Cavoukian, *Privacy by Design: The 7 Foundational Principles*. Office of the Information & Privacy Commissioner of Ontario, 2009.

Ann Cavoukian, *Access by Design: The 7 Fundamental Principles*. Office of the Information & Privacy Commissioner of Ontario, 2010.

Ann Cavoukian, “Privacy Risk Management: Building Privacy Protection into a Risk Management Framework to Ensure That Privacy Risks Are Managed, by Default”, Office of the Information & Privacy Commissioner of Ontario http://www.privacybydesign.ca/publications/accountable-business-practices.

Ann Cavoukian, and Drummond Reed, “Big Privacy: Bridging Big Data and the Personal Data Ecosystem through Privacy by Design” http://www.ipc.on.ca/english/Resources/Discussion-Papers/Discussion-Papers-Summary/?id=1352.

Ann Cavoukian, and Justin Weiss, “Privacy by Design and User Interfaces: Emerging Design Criteria – Keep It User-Centric” http://www.ipc.on.ca/English/Resources/Discussion-Papers/Discussion-Papers-Summary/?id=1201.

Ann Cavoukian, Martin E. Abrams, and Scott Taylor, “Privacy by Design: Essential for Organizational Accountability and Strong Business Practices”, Office of the Information and Privacy Commissioner, Ontario, Canada http://www.ipc.on.ca/images/Resources/pbd-accountability_HP_CIPL.pdf.

Ann Cavoukian, and Terry McQuay, “A Pragmatic Approach to Privacy Risk Optimization: *Privacy by Design* for Business Practices”, NYMITY and the Office of the Information and Privacy Commissioner http://www.ipc.on.ca/english/Resources/Discussion-Papers/Discussion-Papers-Summary/?id=909.

Article 29 Data Protection Working Party. “Opinion 03/2013 on Purpose Limitation.” (2013).

Article 29 Data Protection Working Party. “Opinion 06/2013 on Open Data and Public Sector Information (‘PSI’) Reuse.” (2013).

Article 29 Data Protection Working Part. “Opinion 15/2011 on the definition of consent.” (2011).

Bart Custers, Simone van der Hof, et al. “Informed Consent in Social Media Use: The Gap between User Expectation and EU Personal Data Protection Law.” *Scripted.* 10(4) (2013).

COM(2012) 11/4 Draft 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).

Craig Mundie, "Privacy Pragmatism," *Foreign Affairs*, February 12, 2014, http://www.foreignaffairs.com/articles/140741/craig-mundie/privacy-pragmatism.

Dana Post, "Plaintiffs Alleging Only 'Future Harm' Following a Data Breach Continue to Face a High Bar," *IAPP Privacy Advisor*, January 29, 2014, https://www.privacyassociation.org/publications/plaintiffs_alleging_only_future_harm_following_a_data_breach_continue_to_fa.

Daniel Solove. "Privacy Self-Management and the Consent Dilemma." *Harvard Law Review* 126 (2013): 1879–2139.

Eduardo Ustarian, "The Privacy Pro's Guide to the Internet of Things," *IAPP Dashboard*, February 12, 2014, https://www.privacyassociation.org/privacy_perspectives/post/the_privacy_pros_guide_to_the_internet_of_things.

Fred H. Cate, Peter Cullen, and Viktor Mayer-Schönberger, "Data Protection Principles for the 21st Century: Revising the 1980 OECD Guidelines" http://www.oii.ox.ac.uk/publications/Data_Protection_Principles_for_the_21st_Century.pdf.

Freedom of Information and Protection of Privacy Act, R.S.O. 1990, C. F.31.

Gerrit Hornung, and Christoph Schnabel. *Computer Law & Security Report*. Vol. 25, 2009.

Information and Privacy Commissioner of Ontario (Producer). January 24, 2014. "Big Data Calls for Big Privacy – Not Big Promises" [Video webcast]. Retrieved from http://www.privacybydesign.ca/index.php/webinar-big-data-calls-big-privacy-big-promises/.

ISO/IEC. "29100:2011 Information Technology – Security Techniques – Privacy Framework."

Khaled El Emam. *Guide to the De-Identification of Personal Health Information*: CRC Press, 2013.

Khaled El Emam, and Luk Arbuckle. *Anonymizing Health Data: Case Studies and Methods to Get You Started*: O'Reilly Media, Inc., 2013.

Marc Rotenberg, "Fair Information Practices and the Architecture of Privacy (What Larry Doesn't Get)," *Stanford Technology Law Review*, 1 (2001): 1–4.

Merriam-Webster, "Monetize" http://www.merriam-webster.com/dictionary/monetize.

Merriam-Webster, "Paternalism" http://www.merriam-webster.com/dictionary/paternalism.

Municipal Freedom of Information and Protection of Privacy Act, R.S.O. 1990, C. M.56.

Neelie Kroes, "Online privacy – reinforcing trust and confidence," (speech, Brussels, June 22, 2011), European Union, http://europa.eu/rapid/press-release_SPEECH-11-461_en.htm.

Omer Tene and Jules Polonetsky, Big Data for All: Privacy and User Control in the Age of Analytics, 11 Nw. J. Tech. & Intell. Prop. 239 (2013). http://scholarlycommons.law.northwestern.edu/njtip/vol11/iss5/1.

Organization for the Economic Cooperation and Development (OECD), *The 2013 OECD Privacy Guidelines* (Sept 2013) available at: www.oecd.org/sti/ieconomy/2013-oecd-privacy-guidelines.pdf and Full Privacy Framework: available at: www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf.

Organization for the Economic Cooperation and Development (OECD), "Privacy Expert Group Report on the Review of the 1980 OECD Privacy Guidelines", OECD Digital Economy Papers, No. 229, OECD Publishing (2013). http://dx.doi.org/10.1787/5k3xz5zmj2mx-en.

Paula Bruening, "Data Privacy Day 2014," January 28, 2014, Intel Corporation, http://blogs.intel.com/policy/2014/01/28/today-day-rethink-privacy.

Ryan Calo, "Against Notice Skepticism in Privacy (and Elsewhere)," *Notre Dame Law Review* 87 (2012): 1027–72 http://ssrn.com/abstract=1790144.

Ryan Calo, "The Boundaries of Privacy Harm," *Indiana Law Journal* 86:3 (2011).

Federal Trade Commission (FTC), *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers* (March 2012).

Scott Charney, "Microsoft Trustworthy Computing Next" (V1.01), February 2012, http://www.microsoft.com/en-us/download/details.aspx?id=29084.

Stuart Shapiro, "The Risk of the 'Risk-Based Approach'" *The IAPP Daily Dashboard*, March 31, 2014, https://www.privacyassociation.org/privacy_perspectives/post/the_risk_of_the_risk_based_approach.

Chapter 13
Evolution or Revolution? Steps Forward to a New Generation of Data Protection Regulation

Attila Kiss and Gergely László Szőke

Abstract The birth of data protection regulation in Europe was directly linked to technological developments – mainly to the impressive IT developments of the 70s and their application in public administration. This development has challenged data protection law on every single day ever since. Now, the European data protection law is under revision. One of the most important purposes of the reform is to react to the latest technological developments and to the related social changes once again. The indicated changes are much more than the fine-tuning of the legislation: a new theoretical approach is delineating. The core element of this approach is effectively protecting the individuals' privacy even if their privacy awareness is low, and even if they do not take steps in order to be protected ("invisible protection"). In this paper the key elements of this new generation of personal data protection regulation are shown. Although some aspects of the Proposal for a Regulation will be highlighted in order to underlay our thesis, a complete and detailed analysis of the Proposal cannot be presented within this paper.

13.1 Introduction

The birth of data protection regulation in Europe was directly linked to technological developments – mainly to the impressive IT developments of the 70s, first applied in public administration and later in the business sphere.[1] From the very beginning

This work was partially supported by the European Union and the European Social Fund through "Jól-lét az információs társadalomban" project (grant no.: TAMOP-4.2.2.C-11/1/KONV-2012-0005).

[1] In addition, the very first publication of the right to privacy written by Warren and Brandeis in 1890 was also motivated by the new technology of a camera, which made it possible to take instantaneous photographs. See Samuel D. Warren and Louis D. Brandeis, "The Right to Privacy",

A. Kiss (✉) • G.L. Szőke (✉)
University of Pécs, Pécs, Hungary
e-mail: kiss.attila@ajk.pte.hu; szoke.gergely@ajk.pte.hu

S. Gutwirth et al. (eds.), *Reforming European Data Protection Law*,
Law, Governance and Technology Series 20, DOI 10.1007/978-94-017-9385-8_13

these developments challenged data protection law on a daily basis. Currently, however, European data protection law is undergoing long awaited revision, and one of the most important aims of reform is to react appropriately to the latest technological developments and to the related social changes once more.[2]

The development of data protection legislation over the past 40 years is sometimes described as being consecutive generations of data protection regulation.[3] We, however, share the view of many authors[4] and believe that it is time for a paradigm shift in data protection legislation, since a new generation of regulation is needed. The aim of this paper, therefore, is to draft the key elements of a framework for such a new generation of European data protection, at the same time comparing the European Commission's Proposal for Regulation,[5] as amended by the European Parliament to this concept.[6]

According to our thesis, most of the proposed changes fit into a relatively new philosophical framework, showing that a new approach in the field of data protection has emerged. The essence of this approach is the effective protection of the individuals' privacy, even if their privacy (or generally legal) awareness is low, and even if they take no steps for protection ("background protection"). This approach should not count on activity on the part of the data subjects any more than previously; the emphasis is clearly shifting from the rights of the data subject to the duties of data controllers. This differs greatly from the former philosophical

Harvard Law Review 4 (1890): 195, accessed October 2, 2013, http://heinonline.org/HOL/Page?collection=journals&handle=hein.journals/hlr4&id=205&terms=photograph#207.

[2] Viviane Reding, "The upcoming data protection reform for the European Union," *International Data Privacy Law* 1 (2011): 3, accessed September 12, 2013, doi: 10.1093/idpl/ipq007.

[3] See e.g. Viktor Mayer-Schönberger, "Generational Development of Data Protection in Europe," in *Technology and Privacy: The New Landscape*, ed., Philip E. Agre, Marc Rotenberg (Cambridge, London: MIT Press, 1998), 219–241., and Jóri András, *Adatvédelmi kézikönyv* (Budapest: Osiris, 2005), 22–23.

[4] See e.g. Omer Tene, "Privacy: The new generations," *International Data Privacy Law* 1 (2011): 25–27, accessed September 12, 2013, doi: 10.1093/idpl/ipq003. and Yves Poullet, "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 (Springer, 2010), 3–30. A quite different approach is shown by Burkert, see Herbert Burkert, "Towards a New Generation of Data Protection Legislation," in *Reinventing Data Protection?,* ed. Serge Gutwirth et al. (Springer, 2010), 335–342.

[5] 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,"* COM(2012) 11 final, hereinafter "Commission's Proposal".

[6] European Parliament, *"European Parliament legislative resolution of 12 March 2014 on the 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)0011–C7-0025/2012–2012/0011(COD)), accessed June 30, 2014, http://www.europarl.europa.eu/sides/getDoc.do?type=TA&language=EN&reference=P7-TA-2014-0212 hereinafter "Proposal", or "Parliament's Proposal". The European Parliament adopted the text as it was proposed by the Committee on Civil Liberties, Justice and Home Affairs (LIBE Committee, Rapporteur: Jan Philipp Albrecht).

background of European privacy protection, which was based on the concept of the "informational self-determination", developed by the German Constitutional Court, still heavily influencing data protection regulation in Europe.

In the first part of the paper a historical overview will be sketched in order to show how the evolution of data protection law was led by technological development. Secondly, the key elements of a new generation of personal data protection laws are introduced with respect to the Proposal for a new Data Protection Regulation.[7]

13.2 Historical Background and Current State of Affairs

In the 70s the development of information technology made it possible to apply computers to operate state-owned databases, and so personal information could be controlled by means of these digitalized databases much more rapidly, and different state registers could be merged and connected, showing many aspects of an individual's life; it was even possible to create personality profiles based on these.

Although some major companies had started to introduce computerized databases processing personal data, the real threat to privacy at this time was connected to data processing by the state, often referred to as the 'Big Brother' effect based on Orwell's famous novel '1984'. These concerns drove the first data protection law in the world to be enacted in the *Land* of Hesse, Germany in 1970. This Act "set the course for all further discussions"[8] and served as an example for the legislation enacted in many West European states (Sweden: 1973, Germany: 1976, Denmark, Norway France: 1978, etc.).[9]

Data protection Acts of the 70s, sometimes referred to as the first generation of data protection regulation, were enacted in a world where few data controllers (mostly government bodies and some major companies) used automated data processing technology, and where the general purpose was to limit the state's power by ensuring the transparency of the state's databases.[10]

In the 80s and 90s the world changed a great deal – also from the perspective of privacy risks. Various developments such as the spread of personal computers (first as standalone computers, later connected by the Internet),[11] the wide-spread

[7] Although some features of the Proposal for a Regulation will be highlighted in order to support our thesis, the scope of this paper does not cover a complete and detailed analysis of the Proposal.

[8] Spiros Simitis, *The Hessian Data Protection Act* (Wiesbaden: The Hessian Data Protection Commissioner, 1987), 5.

[9] Herbert Burkert, "Privacy – Data Protection. A German/European Perspective," in *Governance of Global Networks in the Light of Differing Local Values,* ed. Christoph Engel and Kenneth H. Keller (Baden-Baden: Nomos, 2000), 48–50. accessed October 10, 2013, http://www.coll.mpg.de/sites/www.coll.mpg.de/files/text/burkert.pdf.

[10] Jóri András, *Adatvédelmi kézikönyv*, 24–25.

[11] Robert Hassan, *The Information Society* (Cambridge: Polity Press, 2008), 3.

usage of computers in the business sphere, the new (direct) marketing techniques, and, still later, the development of online marketing (based on cookies and other tracking methods),[12] as well as the increasing importance of customer relationship management (CRM) and enterprise resource planning (ERP), made evidenced that demand from the business sphere (sometimes referred to as "Little Brother") for personal data is at least as significant as a state's "natural intention" to collect personal data.

Later, from the middle of the 90s, the rapid expansion of Internet usage and the appearance of many online services set new challenges for regulators. The establishment of the "information society" became a political programme in the European Union, and so documents were adopted in this field, all emphasising the importance of privacy. As ensuring the legal protection of personal information plays an important role also in building trust in the field of online services, its legal regulation, and, in a broader sense, the entire privacy issue of the Internet became an important element of this broadened and vaguely defined phenomenon referred to as the "information society".[13] Another significant trend at this time was the globalization of data processing, which generated the significant feature of trans-border data flow, so creating the need for international and European regulation.[14]

Considering the challenges to be faced and the general trends of the decade, it can be argued that the data protection legislation introduced reflected them quite well. The focus of the regulation extended from governments to new subjects, to companies and organizations. In parallel, international and European laws were adopted which assured, or at least attempted to assure, the legal certainty of international data flows,[15] to strengthen the rights of the data subjects' and to introduce some new approach to legislation. One of the most important new concepts was developed by the German Constitutional Court in 1983, the concept of informational self-determination. This should be understood as "the authority of the individual to decide himself, on the basis of the notion of self-determination, when and within what limits information about his private life should be communicated to others".[16] However this right cannot be unlimited as the data subject has to accept

[12] Joseph Turow and Nora Draper, "Advertising's new surveillance ecosystem," in *Routledge Handbook of Surveillance Studies,* ed. Kirstie Ball, Kevin D. Haggerty and David Lyon (London: Routledge), 134–135.

[13] For a summary on Information Society issues in the EU please consult: "Information society," accessed October 10, 2013, http://europa.eu/legislation_summaries/information_society/index_en.htm.

[14] Some international incidents concerning international data transfers in Europe also clearly showed the necessity for international/European regulation. See Burkert, "Privacy – Data Protection" 51. 53.

[15] See in detail Burkert, "Privacy – Data Protection," 51–53.

[16] Antoinette Rouvroy and Yves Poullet, "The Right to Informational Self-Determination and the Value of Self-Deployment: Reassessing the Importance of Privacy for Democracy," in *Reinventing Data Protection?,* ed. Serge Gutwirth et al. (Springer, 2010), 45.

limitations in the case of overriding general interest when this is incorporated into a law and is clear and proportional.[17]

Although European countries followed different value approaches in the development of national data protection rules,[18] the concept of informational self-determination strongly affected the European data protection regimes,[19] and the data subjects' control and the consent (as legal ground for data processing) became a key issue: "The notion of consent is traditionally linked with the idea that the data subject should be in control of the use that is being made of his data. [. . .] Consent is related to the concept of informational self-determination."[20] Consent has played an important role in conceptions of data protection and privacy. At the same time, it shows that consent has not been deemed as the only legal ground for legitimising data processing operations.[21]

During the last 10–15 years, there have been further significant social, economic and cultural changes which EU legislation has had to face and respond to, and the Proposal for a Regulation can be seen as a milestone in this process. Its new trends have been summarised by many authors, some of whom highlight the role of Web 2.0 technologies, which clearly has had a great effect on privacy. On the one hand, it seems, that people like to "post and search for personal, often intimate, information online" about themselves, and so legislation has to focus on a "new generation of users",[22] whose attitude to privacy may be different from that of earlier generations.[23] On the other hand, user generated content may result in millions of users being regarded as data controllers,[24] and so they are subjects of data protection legislation – but with some of the responsibilities imposed on data controllers.

Some other trends should also be highlighted, such as ubiquitous computing, and the "internet of things",[25] the growing importance of cloud computing, mobile data processing (including location tracking and third party applications), smart

[17] Burkert, "Privacy – Data Protection" 54.

[18] Burkert, "Privacy – Data Protection" 53–56.

[19] And it has had a significant effect on the Hungarian development of data protection law. Jóri András, *Adatvédelmi kézikönyv,* 27.

[20] Article 29 Data Protection Working Party, *"Opinion 15/2011 on the definition of consent,"* 8. accessed September 22, 2013, http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp187_en.pdf.

[21] Article 29 Data Protection Working Party *"Opinion 15/2011 on the definition of consent,"* 5–6.

[22] Tene, "Privacy: The new generations," 15, 21.

[23] Although it is not true that youth does not care about privacy. Empirical research shows the contrary. See Tene, "Privacy: The new generations," 23.

[24] Brendan Van Alsenoy, Joris Ballet, Aleksandra Kuczerawy and Jos Dumortier, "Social networks and web 2.0: are users also bound by data protection regulations?" *Identity in the Information Society* 1 (2009): 70, accessed October 4, 2013, doi: 10.1007/s12394-009-0017-3.

[25] Neil Robinson, Hans Graux, Maarten Botterman and Lorenzo Valeri, *Review of the European Data Protection Directive,* (RAND Europe), 16–17. accessed February 12, 2014, http://www.rand.org/content/dam/rand/pubs/technical_reports/2009/RAND_TR710.pdf.

grid, robotics personalized medicine and biometrics.[26] The spread of sophisticated methods of profiling,[27] and the new technologies of marketing (mostly behavioural advertising) should also be mentioned.

It seems that current legislation cannot respond to these challenges. Many critical opinions have been published in the past few years – and voices heard urging significant changes or a new generation of regulation to appear.[28] Both technology and users have changed much, and so these trends clearly call for a new data protection regime, new laws with new concepts, precisely as in the 70s and, later, in the 90s. In our view, the Proposal for a Regulation indicates significant change and broadly meets the criteria for a new generation of regulation.

13.3 Key Elements of a Framework for a New Generation of Data Protection

Several public opinion surveys have recently focused on the individual's approach to the processing of their personal data and the role of their (informed) consent. According to the latest results, average internet users tend to think that their privacy is threatened in a variety of ways when browsing the Internet or using online services[29] and mainly express privacy-protectionist attitudes.[30] Only 35 % of the respondents consider the selling of their personal data by data controllers acceptable, even with their permission, and yet the sharing of their information with third parties was judged unacceptable by 52 %.[31]

Nevertheless, either this opinion rarely affects their actual behaviour, or there is a lack of understanding of the possible consequences.[32] The CONSENT project found

[26] Tene, "Privacy: The new generations," 16–20.

[27] About the variety of applications of profiling see Mireille Hildebrandt and Serge Gutwirth, ed., *Profiling the European Citizen. Cross Disciplinary Perspectives*, (Springer, 2010).

[28] Among many others, see: Robinson, Graux, Botterman and Valeri, *Review of the European Data Protection Directive,* 38–39., Tene, "Privacy: The new generations," 25–27., Reding, "The upcoming data protection reform for the European Union,".

[29] Noellie Brockdorff and Sandra Appleby-Arnold, "What Consumers think" (paper presented at Online Privacy: Consenting to your Future International Conference, Malta, March 20–21, 2013): 9–10, accessed January 28, 2014, http://consent.law.muni.cz/storage/1365167549_sb_consentonlineprivacyconferencemarch2013-consentprojectresultswhatconsumersthink.pdf. See further results of the CONSENT project at http://consent.law.muni.cz.

[30] Miriam J. Metzger, "Effects of Site, Vendor, and Consumer Characteristics on Web Site Trust and Disclosure," *Communication Research* 33 (2006): 168, accessed February 12, 2014, http://netko.informatika.uni-mb.si/mcnet/upload/attachments/marko_ivan/E-business.pdf.

[31] Brockdorff and Appleby-Arnold, "What Consumers think", 12.

[32] Bart Custers, et al., "Informed Consent in Social Media Use – The Gap between User Expectations and EU Personal Data Protection Law" *SCRIPTed* 10 (2013): 442, accessed February

that only 24 % read privacy policies, even if they are aware of their presence,[33] contrary to the earlier results of EUROBAROMETER which showed 58 %.[34] Moreover, only seven out of ten European reading privacy policies on a regular basis adapted their behaviour on disclosing personal information.[35]

In addition, we should also mention that online service providers often publish their privacy policies as part of the general terms of use, and so these are "take it or leave it" conditions for users. Although users can, theoretically, choose another service provider, they usually want to use one particular service (often because of the so-called network effect), and so they may accept the general terms and the privacy policy automatically, without any consideration. An increased need for self-disclosure can also be seen, as many individuals tend to share their low-sensitive personal data for little in the form of economic benefit, or even free of charge.[36] Meanwhile, users with more control over their personal information, and better personal data management, seem to allow more use of their data.[37] According to the results of projects investigating this issue, individuals tend to think that general social security, which they are used to in the offline context, is also guaranteed for their privacy online, and individuals mask their perceived lack of control over their personal data as a lack of interest in their privacy.[38]

In a more general context, the data subject may be often regarded as the weaker party, and "data subjects are often at risk of inadvertently losing control over their personal information when dealing with those on whom they depend for the provision of jobs, information, goods or services." The power imbalance is likely to enable the stronger party "to use its power to effectively force [data subjects] to consent to certain processing activities."[39]

Due to these trends, a new generation of data protection legislation is needed with a new philosophical approach. The essence of the new regime will be to effectively protect individual privacy, even if their privacy awareness is low, and even if they do

12, 2014, http://script-ed.org/wp-content/uploads/2013/12/custers_et_al.pdf and Kristina Irion and Giacomo Luchetta, "Online personal data processing and EU data protection reform" (Brussels: Centre for European Policy Studies, 2013), 39, accessed October 16, 2013, http://www.ceps.eu/book/online-personal-data-processing-and-eu-data-protection-reform.

[33] Brockdorff and Appleby-Arnold, "What Consumers think", 17–18.

[34] "Special Eurobarometer 359. Attitudes on Data Protection and Electronic Identity in the European Union," 2011, 112, accessed 17 October, 2013. http://ec.europa.eu/public_opinion/archives/ebs/ebs_359_en.pdf.

[35] "Special Eurobarometer 359", 115.

[36] The Boston Consulting Group, *The Value of Our Digital Identity* (Liberty Global Policy Series, 2012), 13, accessed February 12, 2014, http://www.libertyglobal.com/PDF/public-policy/The-Value-of-Our-Digital-Identity.pdf.

[37] The Boston Consulting Group, *The Value of Our Digital Identity,* 15.

[38] Brockdorff and Appleby-Arnold, "What Consumers think", 28–29.

[39] Judith Rauhofer, "One Step Forward, Two Steps Back? Critical observations on the proposed reform of the EU data protection framework," *Journal of Law and Economic Regulation,* 1 (2013): 62.

not take any steps to be protected by ensuring so-called “background protection”. The new data protection regime should not count on the data subject’s activity any more than previously; the emphasis is clearly shifting from the rights of the data subject to the (accountable) duties of the data controllers.[40]

This approach may be similar to that followed by consumer protection,[41] which also aims to protect the weaker party. This, for example, includes ‘blacklisting’ (a practice invariably regarded as unfair) which should trigger action by a strong consumer protection authority or NGOs. This means that, although freedom of contract is a generally important principle, but even if the consumer ignores the general terms and conditions, the authorities do not, and so consumers cannot enter into a totally unfair contract.[42]

In this chapter the core elements of this new model of data protection regulation will be sketched, whilst comparing the proposed provisions of the proposed GDPR to this model.

13.3.1 Shift in Regulation to the Compliance Responsibilities of Data Controllers

13.3.1.1 The Main Features of This Trend

Increasing the accountability of data controllers is an important issue in professional debate on the future of data protection regulation. The principle of accountability was expressed in detail in the opinion 3/2010 of Article 29 of the Working Party,[43] and it arose again in the Commission’s Communication on “a comprehensive approach on personal data protection in the European Union”, which was one of the preparatory documents of the new data protection proposal. In both of these documents the approach to the principle was quite cautious: accountability was interpreted as a general principle, which does not impose cumbersome new legal requirements, but “aims at ensuring de facto, effective compliance with

[40] This does not mean, in our view, that the rights of the data subjects and/or the regulation of consent should be weakened, indeed, they should be kept, and detailed provisions concerning the realization of current rights would be useful, although it is unlikely that strengthening these rights would significantly increase the actual level of privacy protection.

[41] A similar approach is followed in many other sectors, e.g. food or any other product safety regimes.

[42] About the possible comparison parallel between future data protection rules and consumer protection rules, see also Rauhofer, “One Step Forward, Two Steps Back?” 84.

[43] Article 29 Data Protection Working Party, *“Opinion 3/2010 on the principle of accountability,”* accessed February 22, 2014, http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp173_en.pdf.

existing ones".[44] According to the Commission, the principle "would not aim to increase [. . .] administrative burden on data controllers, since such measures would rather focus on establishing safeguards and mechanisms which make data protection compliance more effective".[45] Besides this both of these documents mention (as "illustration") some accountability measures, e.g. drawing up written policies, carrying out a data protection impact assessment, setting up internal procedures to handle complaints, appointing data protection officers, etc.[46]

In our view these measures should be prescribed as legal requirements for some data controllers, whilst admitting that these are very concrete duties for data controllers which impose administrative burdens and cost – even if they are not new principles, but measures to ensure the realization of existing ones. These compliance costs may be regarded as investment for building trust in online services, which seems to be a key factor in the development of the online business sector.

The Proposal for Regulation clearly takes significant steps in this direction. In order to confirm this statement, some provisions of the new Proposal on the data controllers' duties and on the rights of data subjects are reviewed and assessed.

13.3.1.2 Duties of Data Controllers/Data Processors Under the Proposed GDPR

The Proposal for a Regulation contains a variety of (new) obligations for data controllers. Further, a brief summary of the main points relating to these obligations will be provided.[47]

1. The sections entitled "Responsibility and accountability of the controller" shows a general approach regarding data controller's responsibilities, and they make it the controller's task to adopt appropriate policies (codes of practice, rules) and to take all reasonable steps to implement compliance policies.[48] Apart from this, the data controller should be able to demonstrate the adequacy and effectiveness of these measures.[49]

[44] Article 29 Data Protection Working Party, *"Opinion 3/2010 on the principle of accountability,"* 10.

[45] European Commission, *"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,"* COM (2010) 609 final, point 2.2.4.

[46] Article 29 Data Protection Working Party, *"Opinion 3/2010 on the principle of accountability,"* 11–12., European Commission, *"Communication on a comprehensive approach on personal data protection in the European Union,"* point 2.2.4.

[47] For further analysis regarding the obligations imposed on data controllers see also: Szőke Gergely László, "Self regulation, audit and certification schemes in the field of data protection," in *Privacy in the Workplace. Data Protection Law and Self-Regulation in Germany and Hungary*, ed. Szőke Gergely László (Budapest: HVG-ORAC, 2012). 289–292.

[48] Proposal for a Data Protection Regulation, Article 22, 1-1a.

[49] Proposal for a Data Protection Regulation, Article 22, 3.

2. The Proposal for a Regulation lays down an obligation for data controllers/processors to maintain regularly updated documentation containing basic information about the data processing carried out.[50] Some further requirements proposed by the Commission concerning the content of the documentation have been moved to Article 14 on information rights in the Parliament's Proposal, in order to merge information and documentation, "essentially being two sides of the same coin."[51] According to Article 13a data controllers shall also provide some standardized information about data processing using well-defined pictograms.[52]

   All things considered, the data controllers need to catalogue each of his processing operations one by one in order to ensure the duties to maintain documentation and provide information.
3. Article 30 (1) relating to data security measures imposes on data controllers an obligation which basically corresponds to the provisions of the currently effective Directive, supplementing it with the condition that the data controller shall take these measures "taking into account the results of a data protection impact assessment".[53] As a novelty, Article 30 (1a) prescribes some compulsory elements of a security policy. This means that, contrary to the current regulation, data controllers and processors should adopt (written) security policies to comply with these provisions.
4. The Proposal for a Regulation lays down for all data controllers the obligation to carry out a risk analysis of the potential impact of the intended data processing.[54] If specific risks are likely to be presented by the data processing, the controllers shall also carry out data protection impact assessment and periodical compliance review.[55] The Parliament's Proposal lists the circumstances of data processing operations which are likely to present specific risks; e.g. processing of more than 5,000 data subjects' personal data, or processing special categories of personal data (sensitive data), or profiling, if it has legal effects on data subjects, automated monitoring of publicly accessible areas on a large scale (like CCTV systems), etc.

   It may be concluded that the obligation to carry out data protection impact assessment concerns a well-defined, but somewhat wide range of data controllers: anyone with more than 5,000 clients, CCTV system operators, health care system institutions, political and religious organizations – to mention a few.

[50] Proposal for a Data Protection Regulation, Article 28, 1–2.

[51] Committee on Civil Liberties, Justice and Home Affairs (Rapporteur: Jan Philipp Albrech), Draft Report on the proposal for a regulation of the European Parliament and of the Council on the protection of individual with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), (COM(2012)0011–C7-0025/2012–2012/0011(COD)), accessed October 2, 2013 http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/pr/922/922387/922387en.pdf, p. 86.

[52] Proposal for a Data Protection Regulation, Article 13a.

[53] Proposal for a Data Protection Regulation, Article 30.

[54] Proposal for a Data Protection Regulation, Article 32a.

[55] Proposal for a Data Protection Regulation, Article 32a, 3. (c), Article 33a.

5. Compared to the present situation a significant additional obligation is imposed on data controllers by prescribing "data breach notification" – applicable under the effective European rules only to service providers in the telecommunications sector. Its essence lies in the fact that, in the case of a breach of the rules relating to personal data[56] the data controller is obliged to notify the authority and also, in some cases, those concerned.
6. In accordance with Article 35 of the Parliament's Proposal, the controller and the processor shall appoint a data protection officer in any case where

   - the processing is carried out by a public authority or body, or
   - processing is carried out by a legal person and relates to more than 5,000 data subjects in any consecutive 12 month period, or
   - the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects, or
   - the core activities of the controller or the processor consist of processing special categories of data, location data or data on children or employees in large scale filing systems.

The aim of presenting these six points of the planned new regulation in detail was to demonstrate, that these provisions, compared to the current regulation, impose considerable additional duties on data controllers. Complying with them will demand significant efforts from data controllers, and will generate considerable compliance costs.[57]

In our view, the proposed measures are suitable for ensuring the accountability principle, and will increase the actual level of privacy protection. This will arise, firstly, by enhancing the awareness of data controllers, so reducing unwanted or unnecessary data processing operations, and, secondly, by improving the transparency of data processing, which may be controlled by data subjects, and so (most importantly) making the tasks of data protection authorities and NGOs easier.

13.3.2 Distinguishing the Duties of Data Controllers

13.3.2.1 The Main Features of the Trend

Once regulations impose new requirements on data controllers, we need to be able to distinguish among them in several ways. As Article 29 of the Working Party

[56] "Personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed". Commission's Proposal for a Data Protection Regulation, Article 4, 9.

[57] Domokos Márton, "Az EU új adatvédelmi szabályozásának várható következményei a gyakorlatban," *Infokommunikáció és jog*, 2 (2013): 58.

emphasises, the "one-size-fits-all" approach should be avoided, and, rather, the "specific measures to be applied must be determined, depending on the facts and circumstances of each particular case, with particular attention to the risk of the processing and the types of data."[58]

There are two main reasons for differentiating the duties of data controllers. First, it is important to avoid unnecessary administrative burdens and costs and the (potential) decrease in the competitiveness of smaller businesses processing a low volume of personal data, or processing personal data only as an activity ancillary to its main activities. Second, as mentioned above, millions of users can also be regarded as data controller in some cases, mostly due to user-generated content. It is crucial to make some difference regarding the duties of the "everyday users", even if they fall within the scope of definition of 'data controller'.

13.3.2.2 The Provisions of the Proposed GDPR

As shown in Sect. 13.3.1.2, some of the duties are only imposed by the GDPR on data controllers if certain criteria are met. The Proposal tries to summarize these criteria under the broad category of "Data processing likely to present a specific risk". First of all, all data controllers should carry out a risk analysis to show if their data processing meets any of the following criteria:

1. processing of personal data relating to more than 5,000 data subjects (during any continuous 12-month period),
2. processing of special categories of personal data, location data or data on children or employees in large-scale filing systems,
3. profiling, if it produces legal (or similarly significantly) effects on the individual,
4. processing of personal data for the provision of health care, epidemiological research, or surveys of mental or infectious diseases, where the data are processed for taking measures or decisions regarding specific individuals on a large scale,
5. automated monitoring of publicly accessible areas on a large scale,
6. other processing operations for which the consultation of the DPO or supervisory authority is required,
7. where a personal data breach would likely adversely affect the protection of the personal data, the privacy, the rights or the legitimate interests of the data subject,
8. the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects,
9. where personal data are made accessible to a number of potentially unlimited persons.[59]

[58] Article 29 Data Protection Working Party, *"Opinion 3/2010 on the principle of accountability,"* 13.

[59] Proposal for a Data Protection Regulation, Article 32a, 2.

The Proposal then imposes some of the duties only on data controllers who meet certain criteria, e.g. data protection impact assessment needs only to be carried out if any of the criteria in points 1–8 are met, and the appointment of a DPO is only compulsory in cases detailed in points 1–2 and 8.[60]

In our view, the list is quite problematic: while some of the criteria are objective and clear, and so the data controller can decide whether their data processing fulfils that particular requirement, the others are too general, and cannot easily be interpreted by data controllers – particularly, the requirement in point 7 is hard to interpret. Generally, it would seem that the circumstances and the duty to carry out a data protection impact assessment will apply to too wide a range of data controllers.

13.3.3 Regulating the Technology

Given the fact that European data controllers are obliged to process personal data in line with all principles of the Directive in force and will have to face a number of new duties in the planned legal framework, the use of technologies which foster the legitimate processing of data could effectively reduce the costs of meeting the obligations and the chance of being sanctioned for illegal data processing activities.[61] On the other hand, it was presented that data subjects see risk in the processing of their personal data, but often practice their rights for informational self-determination irrationally,[62] and so applying technologies which protect their rights automatically could enhance their confidence and trust in these services. Technology can jointly enhance the level of data security, and increase the level of protection of personal information by setting the protection of personal data as 'default' in different services, as a result making their use one of the key elements of a suggested new European legislation. Introducing Privacy by Design (PbD) to the personal data protection regulation will play a major role in forming a new legal framework – not only in the European Union, but also in Canada and the US.[63] PbD has several definitions, but, it refers mainly to the concept that information and communications technologies and systems should be designed (and also operated) as taking privacy into account, even from the outset, as a default setting.

Research interest in shaping technology itself by regulation was generated only in the 90s,[64] largely based on the work of Ann Cavoukian, who defined the aim,

[60] Proposal for a Data Protection Regulation, Article 32a, 3. (b), (c).

[61] Ira S. Rubinstein, "Regulating Privacy by Design." *Berkeley Technology Law Journal* 26 (2012):1411.

[62] Irion and Luchetta, "Online personal data processing and EU data protection reform", 39.

[63] Rubinstein, "Regulating Privacy by Design.", 1411.

[64] Simon Davies, "Why Privacy by Design is the next crucial step for privacy protection," 2010, 1, accessed October 16, 2013, http://www.i-comp.org/blog/wp-content/uploads/2010/12/privacy-by-design.pdf.

the functioning and the effects of Privacy Enhancing Technologies (PETs) and later PbD. The fact that the aims of PbD and the goals of PETs are both connected to the technological background of data processing can be misleading, but they are not synonyms. Despite the overlap in respect of their usage PETs are clear engineering approaches which focus on the positive potential of technology, on tools used to maintain anonymity, confidentiality, or control over personal information,[65] whilst PbD is a broader concept comprising several elements[66] to balance technologies with a framework highlighting the process and their fundamental components.[67] In this sense, PbD is the next step in the evolution of the privacy dialogue.[68]

The recognition that surveillance had become an embedded design component of systems and devices operated by the state or by private organizations led to the spread of PETs. Businesses found their own technical solutions more effective than publicly driven privacy regulation,[69] even though the risk produced by technologies was answered with renewed trust in technology, and resulted in the fact that "risk connected to data processing is moved away from the regulatory authorities, becoming a consumer responsibility entirely."[70]

The first law introducing the privacy regulation by technology (and by PETs) principle was the German Teleservices Data Protection Act of 1997,[71] although most European data controllers still have no obligation to provide technical means of restricting the collection of users' personal data.[72] Therefore, the European Commission and the Article 29 Working Party aim to ensure that the PbD principle is deployed also by controllers and data subjects,[73] embedded in all areas as an appropriate answer to the "collect before select" behaviour.[74]

[65] Rubinstein, "Regulating Privacy by Design.",1412.

[66] Ann Cavoukian, "Privacy by Design, The 7 Foundational Principles," 2011 accessed October 16, 2013, http://www.ipc.on.ca/images/resources/7foundationalprinciples.pdf.

[67] Martin Rost and Kirsten Bock, "Privacy by Design and the New Protection Goals," 2011, 1, accessed October 16, 2013, https://www.european-privacy-seal.eu/results/articles/BockRost-PbD-DPG-en.pdf.

[68] Davies, "Why Privacy by Design is the next crucial step for privacy protection".

[69] Christopher T. Marsden, "Beyond Europe: The Internet, Regulation, and Multistakeholder Governance – Representing the Consumer Interest?" *Journal of Consumer Policy*, 31, (2008): 124.

[70] Dag Slettemeås, "RFID – the "Next Step" in Consumer – Product Relations or Orwellian Nightmare? Challenges for Research and Policy," *Journal of Consumer Policy*, 32, (2009): 238.

[71] Act on the Protection of Personal Data Used in Teleservices (Gesetz über den Datenschutz bei Telediensten), Federal Law Gazette (Bundesgesetzblatt) 1997 I 1871. 3§ (4).

[72] Jan Paul Kolter, *User-Centric Privacy. A Usable and Provider-Independent Privacy Infrastructure* (Lohmar-Köln: JOSEF EUL VERLAG, 2010), 2.

[73] Irion and Luchetta, "Online personal data processing and EU data protection reform", 63.

[74] Hielke Hijmans, "Recent developments in data protection at European Union level," 2010, 222, accessed October 16, 2013, http://link.springer.com/content/pdf/10.1007%2Fs12027-010-0166-8.pdf.

Article 23 of the Proposal clarifies this new type of liability and prescribes that controllers implement appropriate and proportionate technical and organisational measures and procedures ensuring the protection of the rights of the data subject. The draft of the Commission also provided the option to take into consideration the cost of implementation, in contrast to the wording of the Parliament's Proposal, where this option was replaced by the obligation of risk analysis.

As the majority of data processors have not yet embraced the concept of Privacy by Default, the Proposal also adopted this similar principle ensuring automatic protection of data if there is a possibility to choose, in order to achieve better results by preventing the misuse of personal data than by trying to repair any damage caused and 'bolting the stable door' too late.[75] Compliance with the principle of "privacy by design" needs significant effort by data controllers and presupposes that they consciously think over and plan their individual data processing operations and that, already during planning, they are concerned with fulfilling data protection and data security requirements ("entire lifecycle management of personal data").

For the sake of a clear debate on how the concept of PbD relates to certain technologies or organizational measures, or of questions about what the proposed legal obligation implies in practice for the organization's future legislation, the Commission proposed to be empowered to adopt delegated acts based on the Regulation. However, the European Parliament also amended Article 23 of the Proposal in connection to the delegated rights and would empower the European Data Protection Board to specify requirements for these measures and lay down technical standards for Privacy by Design and by Default.[76]

We should also point out as a conclusion, in respect of the role of technology, that these principles ease the compliance duties of data controllers – which leads to the better protection of data subjects, even given their inactivity or lack of interest in privacy. Setting strict rules for data controllers on applying technologies for personal data processing fits the concept of a paradigm shift; it can be seen as a change in balancing responsibilities from the data subjects' informational self-determination towards automatic protection.

13.3.4 Strengthening the National Data Protection Authorities

It should first be stated that data protection authorities (DPAs) operate in all Member States of the EU and their objectives of enforcement are very similar due to the implementation of Directive 95/46/EC. Data controllers may face severe sanctions in cases of a breach of personal data regulations under national laws,

[75] Rubinstein, "Regulating Privacy by Design.",1410–1412.

[76] Proposal for a Data Protection Regulation, Article 30, 3.

but those consequences are not always sufficiently transparent or standardized, and the costs of non-compliance and methods of enforcement can differ significantly.[77] In countries such as France, Germany or Hungary, DPAs have the power to issue substantial fines,[78] and in some, to be more incentivised, authorities even have to recover their own operational costs. On the other hand, there are countries where both the judicial system has to enforce the protection of privacy and impose fines, or others, where legal regimes issue only warnings to data controllers, or ban the processing of certain data.[79]

The other key role of DPAs in this diverse system is to raise public awareness on data protection issues and promote the right to informational self-determination. Despite the wide range of promotional activities undertaken,[80] 63 % of Europeans have never heard of any authority responsible for protecting their personal data,[81] 44 % of citizens would like the enforcement of their rights connected to personal data protection to be dealt with at EU level,[82] whilst 75 % of those surveyed rated laws and authorities preventing the misuse of their data as not strong enough.[83] These results show that the majority of data subjects feel no real opportunity to obtain legal remedy in the case of a breach of the law – due to a lack of knowledge and to the increasing challenges brought by the convergence of social, mobile and cloud computing technologies. In cases of international data leaks, such as the hacked databases of credit card providers and online stores, where the rights of a massive number of citizens are infringed and where breaches may remain hidden from the data subjects, their rights for informational self-determination

[77] European Union 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* (Luxembourg: Publications Office of the European Union, 2010), 34.

[78] "Data protection enforcement in UK, France and Germany explained" accessed 17 October, 2013. http://www.out-law.com/en/articles/2013/july/data-protection-enforcement-in-uk-france-and-germany-explained/.

[79] Neil Robinson et al. *Review of the European Data Protection Directive*, 2009, 36, accessed 17 October, 2013. http://www.ico.org.uk/upload/documents/library/data_protection/detailed_specialist_guides/review_of_eu_dp_directive.pdf.

[80] KANTOR Management Consultants S.A. et al., *Evaluation of the Means used by National Data Protection Supervisory Authorities in the promotion of personal Data Protection. Final Report*, 2007, 16, accessed October 17, 2013, http://ec.europa.eu/justice/policies/privacy/docs/studies/final_report_kantor_management_consultants.pdf.

[81] "Special Eurobarometer 359", 174.

[82] "Special Eurobarometer 359", 184.

[83] The Economist Intelligence Unit, "Privacy Uncovered. Can private life exist in the digital age?," 2013, 23, accessed October 17, 2013. http://www.managementthinking.eiu.com/sites/default/files/downloads/Privacy%20uncovered_0.pdf.

are clearly insufficient. It also leads to the complex problem of assigning the value of any damage to each individual and of judging the responsibilities of data controllers.[84,85]

Under the planned new generation of rules, all DPAs should use a proactive approach, and so be aided in putting privacy laws into effect by the right to impose fines in a unified enforcement system.

The Proposal also faces a challenge by the cooperation of DPAs under the European Data Protection Board, which is assigned the task of taking legally binding decisions upon each DPA of the Member States to guarantee the unified understanding of the rules.[86]

Whilst there is still a great need for the educational and promotional activities of DPAs to foster a culture of privacy (especially among the youth),[87] the new framework of the Proposal would also be applicable as to guard the rights of those European citizens who have less knowledge of the protection of their privacy. To face their new role and the obligations set by Article 39 (1a–1g) of the Parilament's Proposal, it is quite possible that the main tasks of DPAs will be to initiate official procedures to supervise and audit the compliance of data controllers and to play an effective role in data protection law enforcement.

13.3.5 Enhancing Self-Regulation, Audit, and Certification Schemes

Once the compliance tasks of data controllers are increased, the role of internal regulation, self-regulation and various certification schemes are expected to increase. Independent, third- party audits and certification may demonstrate the data controllers' commitment to respecting privacy.

The Proposal for a Regulation contains some advanced provisions in this field. It basically provides specification for the creation of codes of conduct similarly to the regulations contained in the Directive,[88] however, at the same time, it is a novelty that the Proposal incorporates an article on data protection certification and seals. The Parliament's Proposal grants the right for the data controllers to request (on a voluntary basis) any supervisory authority to certify that the processing of personal

[84] Neil Robinson et al. *Review of the European Data Protection Directive*, 2009, 35, accessed 17 October, 2013. http://www.ico.org.uk/upload/documents/library/data_protection/detailed_specialist_guides/review_of_eu_dp_directive.pdf.

[85] Thomas M. Lenard and Paul H. Rubin, "In defense of data: Information and the costs of privacy", 2009, 6, accessed January 28, 2014, http://www.techpolicyinstitute.org/files/in%20defense%20of%20data.pdf.

[86] Proposal for a Data Protection Regulation, Article 55–58.

[87] Proposal for a Data Protection Regulation, Article 52, 2–4.

[88] Proposal for a Data Protection Regulation, Article 38, 1–3.

data is performed in compliance with the Regulation. The supervisory authority may accredit specialised third party auditors to carry out the auditing.[89]

These provisions go much further than the Commission's original draft, according to which – in a rather soft law-type formulation – the Member States and the Commission are to "encourage" the establishment of data protection certification mechanisms and of data protection seals and marks.[90]

13.4 Conclusions

During the last 10–15 years the world has changed a great deal. There were significant technological, social, economic and cultural changes, and the regulation of privacy protection should also face new challenges; new laws with new concepts are needed – precisely as in the 70s and, later, in the 90s.

It would seem that the control actually exercised by data subjects is far not enough, and a new philosophical approach is needed. The core element of this aims at effectively protecting individual privacy, even if privacy awareness is low or in cases where they no steps are taken to be protected – in other words, ensuring a form of "background protection". This approach may be similar to the one followed by consumer protection: the users are provided with much information, and, even if they pay little or no regard to them, a minimum level of protection is ensured, and totally unfair contracts cannot be made.

The many new obligations of data controllers (Sect. 13.3.1) enhance transparency and facilitate the exercise of control both by users, by NGOs and, mostly, by the strengthened (and potentially more active) authorities (Sect. 13.3.4). If these trends are reinforced by intentions to devise and use technology in the service of data protection (Sect. 13.3.3) and with encouragement of data controllers who request certification, so showing their data protection compliance to the public (Sect. 13.3.5), there will be an overall effect or impact – that is, that the actual level of data protection will significantly increase, even without activity on the part of the data subject.

The indicated changes in the field of European data protection legislation show that the EU is trying to face the problems. The Proposal for the GDPR is more relevant than a simple fine-tuning of existing legislation and the focus is clearly shifting to the issues of "what the data controllers shall do", from the question of "what the data subject has the right to". The lobby activities of different organizations and the more than 4,000 amendments to the Commission's draft show that many organizations also consider the proposed changes as a revolution in data protection legislation.

[89] Proposal for a Data Protection Regulation, Article 39, 1a–1g.

[90] The European Commission's Proposal for a Data Protection Regulation, Article 39, 1.

In our view, these changes more or less fit the theoretical model, the main elements of which are sketched in this essay, although some other relevant changes are needed to improve the coherence of the new data protection regime.

Bibliography

Act on the Protection of Personal Data Used in Teleservices (Gesetz über den Datenschutz bei Telediensten), Federal Law Gazette (Bundesgesetzblatt) 1997 I 1871.

Alsenoy, Brendan Van, Joris Ballet, Aleksandra Kuczerawy and Jos Dumortier. “Social networks and web 2.0: are users also bound by data protection regulations?” *Identity in the Information Society* 1 (2009): 65–79. Accessed October 4, 2013. doi: 10.1007/s12394-009-0017-3

Article 29 Data Protection Working Party. *“Opinion 3/2010 on the principle of accountability.”* Accessed February 22, 2014. http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp173_en.pdf

Article 29 Data Protection Working Party. *“Opinion 15/2011 on the definition of consent.”* Accessed September 22, 2013. http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp187_en.pdf

Brockdorff, Noellie and Sandra Appleby-Arnold. “What Consumers think” (paper presented at Online Privacy: Consenting to your Future International Conference, Malta, March 20–21, 2013). Accessed January 28, 2014. http://consent.law.muni.cz/storage/1365167549_sb_consentonlineprivacyconferencemarch2013-consentprojectresultswhatconsumersthink.pdf

Burkert, Herbert. “Towards a New Generation of Data Protection Legislation.” In *Reinventing Data Protection?,* edited by Serge Gutwirth, Yves Poullet, Paul De Hert, Cécile Terwangne and Sjaak Nouwt, 335–342. Springer, 2010.

Burkert, Herbert. “Privacy – Data Protection. A German/European Perspective.” In *Governance of Global Networks in the Light of Differing Local Values,* edited by Christoph Engel and Kenneth H. Keller, 44–69. Baden-Baden: Nomos, 2000. Accessed October 10, 2013. http://www.coll.mpg.de/sites/www.coll.mpg.de/files/text/burkert.pdf

Cavoukian, Ann and Mark Dixon. *Privacy and Security by Design: An Enterprise Architecture Approach.* Ontario: Information and Privacy Commissioner, 2013. Accessed October 15, 2013, http://www.privacybydesign.ca/content/uploads/2013/09/pbd-privacy-and-security-by-design-oracle1.pdf

Cavoukian, Ann, “Privacy by Design, The 7 Foundational Principles.” 2011. Accessed October 16, 2013, http://www.ipc.on.ca/images/resources/7foundationalprinciples.pdf

Committee on Civil Liberties, Justice and Home Affairs (Rapporteur: Jan Philipp Albrecht). *Draft Report on the proposal for a regulation of the European Parliament and of the Council on the protection of individual with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)*, (COM(2012)0011–C7-0025/2012–2012/0011(COD)). Accessed October 2, 2013. http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/pr/922/922387/922387en.pdf

Custers, Bart, Simone van der Hof, Bart Schermer, Sandra Appleby-Arnold and Noellie Brockdorff. “Informed Consent in Social Media Use – The Gap between User Expectations and EU Personal Data Protection Law.” *SCRIPTed* 10 (2013). Accessed February 12, 2014, http://script-ed.org/wp-content/uploads/2013/12/custers_et_al.pdf

Davies, Simon. “Why Privacy by Design is the next crucial step for privacy protection.” Accessed October 16, 2013, http://www.i-comp.org/blog/wp-content/uploads/2010/12/privacy-by-design.pdf

“Data protection enforcement in UK, France and Germany explained.” Accessed 17 October, 2013, http://www.out-law.com/en/articles/2013/july/data-protection-enforcement-in-uk-france-and-germany-explained

Domokos, Márton. "Az EU új adatvédelmi szabályozásának várható következményei a gyakorlatban." *Infokommunikáció és jog*, 2 (2013): 58–63.

European Commission. *"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."* COM (2010) 609 final

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."* COM(2012) 11 final.

European Parliament. *"European Parliament legislative resolution of 12 March 2014 on the 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)0011 – C7-0025/2012 – 2012/0011(COD)), accessed June 30, 2014, http://www.europarl.europa.eu/sides/getDoc.do?type=TA&language=EN&reference=P7-TA-2014-0212

European Union 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.* Luxembourg: Publications Office of the European Union, 2010. Accessed 17 October, 2013. http://fra.europa.eu/sites/default/files/fra_uploads/815-Data-protection_en.pdf

Hassan, Robert. *The Information Society.* Cambridge: Polity Press, 2008.

Hijmans, Hielke. "Recent developments in data protection at European Union level," 2010. Accessed October 16, 2013, http://link.springer.com/content/pdf/10.1007%2Fs12027-010-0166-8.pdf

Hildebrandt, Mireille and Serge Gutwirth, ed. *Profiling the European Citizen. Cross Disciplinary Perspectives.* Springer, 2010.

Irion, Kristina and Giacomo Luchetta. "Online personal data processing and EU data protection reform". Brussels: Centre for European Policy Studies, 2013. Accessed October 16, 2013, http://www.ceps.eu/book/online-personal-data-processing-and-eu-data-protection-reform

Jóri, András. *Adatvédelmi kézikönyv.* Budapest: Osiris, 2005.

KANTOR Management Consultants S.A. et al., *Evaluation of the Means used by National Data Protection Supervisory Authorities in the promotion of personal Data Protection. Final Report*. 2007. Accessed October 17, 2013. http://ec.europa.eu/justice/policies/privacy/docs/studies/final_report_kantor_management_consultants.pdf

Kolter, Jan Paul. *User-Centric Privacy. A Usable and Provider-Independent Privacy Infrastructure.* Lohmar-Köln: JOSEF EUL VERLAG, 2010.

Kuner, Christopher. "The European Commission's Proposed Data Protection Regulation: A Copernican Revolution in European Data Protection Law," *Privacy and Security Law Report,* (2012): 1–15. Accessed October 2, 2013, http://www.ico.org.uk/news/events/~/media/documents/future_of_dp_in_europe_2012/ico_event_future_of_dp_in_europe_2012_Chris_Kuner_article.ashx

Lenard, Thomas M. and Paul H. Rubin. "In defense of data: Information and the costs of privacy". 2009. Accessed January 28, 2014. http://www.techpolicyinstitute.org/files/in%20defense%20of%20data.pdf

Marsden, Christopher T. "Beyond Europe: The Internet, Regulation, and Multistakeholder Governance – Representing the Consumer Interest?" *Journal of Consumer Policy*, 31, (2008): 115–132. Accessed October 2, 2013, doi.10.1007/s10603-007-9056-z

Mayer-Schönberger, Viktor. "Generational Development of Data Protection in Europe." In *Technology and Privacy: The New Landscape*, edited by Philip E. Agre, Marc Rotenberg 219–241. Cambridge, London: MIT Press, 1998.

Metzger, Miriam J. "Effects of Site, Vendor, and Consumer Characteristics on Web Site Trust and Disclosure." *Communication Research* 33 (2006). Accessed February 12, 2014. http://netko.informatika.uni-mb.si/mcnet/upload/attachments/marko_ivan/E-business.pdf

Poullet, Yves. "About the E-Privacy Directive: Towards a Third Generation of Data Protection Legislation?" In *Data Protection in a Profiled World* edited by Serge Gutwirth, Yves Poullet and Paul De Hert, 3–30. Springer, 2010.

Rauhofer, Judith. "One Step Forward, Two Steps Back? Critical observations on the proposed reform of the EU data protection framework." *Journal of Law and Economic Regulation*, 1 (2013): 57–84; Accessed 20 February 2014, http://ssrn.com/abstract=2260967

Reding, Viviane. "The upcoming data protection reform for the European Union." *International Data Privacy Law* 1 (2011): 3–5. Accessed September 12, 2013. doi: 10.1093/idpl/ipq007.

Robinson, Neil Hans Graux, Maarten Botterman and Lorenzo Valeri. *Review of the European Data Protection Directive.* 2009, Accessed 17 October, 2013. http://www.ico.org.uk/upload/documents/library/data_protection/detailed_specialist_guides/review_of_eu_dp_directive.pdf

Rost, Martin and Kirsten Bock. "Privacy by Design and the New Protection Goals." Accessed October 16, 2013, https://www.european-privacy-seal.eu/results/articles/BockRost-PbD-DPG-en.pdf

Rouvroy, Antoinette and Yves Poullet. "The Right to Informational Self-Determination and the Value of Self-Deployment: Reassessing the Importance of Privacy for Democracy." In *Reinventing Data Protection?,* edited by Serge Gutwirth, Yves Poullet, Paul De Hert, Cécile Terwangne and Sjaak Nouwt, 45–76. Springer, 2010.

Rubinstein, Ira S. "Regulating Privacy by Design." *Berkeley Technology Law Journal* 26 (2012): 1410–1456. Accessed October 2, 2013, http://ssrn.com/abstract=1837862

Simitis, Spiros. *The Hessian Data Protection Act.* Wiesbaden: The Hessian Data Protection Commissioner, 1987.

Slettemeås, Dag, "RFID – the "Next Step" in Consumer – Product Relations or Orwellian Nightmare? Challenges for Research and Policy." *Journal of Consumer Policy*, 32, (2009): 219–244. Accessed October 2, 2013, doi.10.1007/s10603-009-9103-z

"Special Eurobarometer 359. Attitudes on Data Protection and Electronic Identity in the European Union." 2011. Accessed 17 October, 2013, http://ec.europa.eu/public_opinion/archives/ebs/ebs_359_en.pdf

Székely, Iván, "The Right to Forget, the Right to be Forgotten." In *European Data Protection: In Good Health?* edited by Serge Gutwirth, Ronald Leenes, Paul De Hert and Yves Poullet, 347–363. Springer, 2012.

Szőke, Gergely László, "Self regulation, audit and certification schemes in the field of data protection," In *Privacy in the Workplace. Data Protection Law and Self-Regulation in Germany and Hungary* edited by Szőke Gergely László, 287–300. Budapest: HVG-ORAC, 2012.

Tene, Omer. "Privacy: The new generations." *International Data Privacy Law* 1 (2011): 15–27. Accessed September 12, 2013. doi: 10.1093/idpl/ipq003.

The Boston Consulting Group. *The Value of Our Digital Identity.* (Liberty Global Policy Series, 2012), Accessed February 12, 2014. http://www.libertyglobal.com/PDF/public-policy/The-Value-of-Our-Digital-Identity.pdf

The Economist Intelligence Unit. "Privacy Uncovered. Can private life exist in the digital age?" 2013. Accessed October 17, 2013, http://www.managementthinking.eiu.com/sites/default/files/downloads/Privacy%20uncovered_0.pdf

Turow, Joseph and Nora Draper. "Advertising's new surveillance ecosystem." In *Routledge Handbook of Surveillance Studies,* edited by Kirstie Ball, Kevin D. Haggerty and David Lyon, 133–140. London: Routledge, 2012

Warren, Samuel D. and Louis D. Brandeis. "The Right to Privacy". *Harvard Law Review* 4 (1890): 195–220. Accessed October 2, 2013. http://heinonline.org/HOL/Page?collection=journals&handle=hein.journals/hlr4&id=205&terms=photograph#207

Chapter 14
Do People Know About Privacy and Data Protection Strategies? Towards the "Online Privacy Literacy Scale" (OPLIS)

Sabine Trepte, Doris Teutsch, Philipp K. Masur, Carolin Eicher, Mona Fischer, Alisa Hennhöfer, and Fabienne Lind

Abstract Empirical research has revealed disparities of internet users' online privacy attitudes and online privacy behaviors. Although users express concerns about disclosing personal data in the internet, they share personal and sometimes intimate details of their and others lives in various online environments. This may possibly be explained by the knowledge gap hypothesis which states that people are concerned about their privacy and would like to behave accordingly, but that lacking privacy literacy prevents them from reacting the ways that they think would most adequately reflect their attitudes and needs. To implement privacy literacy in future research and policy making, a comprehensive scale to measure privacy literacy will be suggested. The online privacy literacy scale (OPLIS) was developed based on an exhaustive review of prior literature on privacy literacy and a profound content analysis of different sources capturing a variety of aspects relevant to online privacy. The scale encompasses five dimensions of online privacy literacy: (1) Knowledge about practices of organizations, institutions and online service providers; (2) Knowledge about technical aspects of online privacy and data protection; (3) Knowledge about laws and legal aspects of online data protection in Germany; (4) Knowledge about European directives on privacy and data protection; and (5) Knowledge about user strategies for individual privacy regulation.

S. Trepte (✉) • D. Teutsch • P.K. Masur • C. Eicher • M. Fischer • A. Hennhöfer • F. Lind
Department of Media Psychology, Institute of Communication Science, University of Hohenheim, Stuttgart, Germany
e-mail: sabine.trepte@uni-hohenheim.de

S. Gutwirth et al. (eds.), *Reforming European Data Protection Law*,
Law, Governance and Technology Series 20, DOI 10.1007/978-94-017-9385-8_14

14.1 Introduction

Online privacy behaviors have been shown to be inconsistent with privacy attitudes.[1,2,3,4] Although users of online services state that they are worried about their personal data,[5,6] they increasingly disclose personal data and intimate stories about their personal lives.[7] This inconsistency has been termed the "privacy paradox".[8] Different rationales for why people's behaviors are not consistent with their beliefs have been provided. A lack of knowledge about how to protect online data is one of the major arguments currently used to explain the gap between online privacy behaviors and online privacy attitudes.[9] It is assumed that users strive to regulate their privacy but have trouble actually doing so due to a lack of online privacy literacy.

In ongoing debates on online privacy, online privacy literacy has been defined as a "principle to support, encourage, and empower users to undertake informed control of their digital identities".[10] It has been stated that making deliberate decisions about online privacy and engaging in informed online privacy behaviors need to be based

[1] Alessandro Acquisti and Ralph Gross, "Awareness, Information Sharing, and Privacy on the Facebook" (Paper presented at the 6th Workshop on privacy enhancing technologies, June 28 – June 30 2006, Cambridge, June 2006).

[2] Stefano Taddei and Bastianina Contena, "Privacy, Trust and Control: Which Relationships with Online Self-Disclosure?," *Computers in Human Behavior* 29, no. 3 (2013).

[3] Sabine Trepte and Leonard Reinecke, "The Social Web as Shelter for Privacy and Authentic Living," in *Privacy Online. Perspectives on Privacy and Self-Disclosure in the Social Web*, ed. Sabine Trepte and Leonard Reinecke (Berlin: Springer, 2011).

[4] Zeynep Tufekci, "Can You See Me Now? Audience and Disclosure Regulation in Online Social Network Sites," *Bulletin of Science*, *Technology & Society* 28, no. 1 (2008).

[5] Eurobarometer, "E-Communications Household Survey," ed. Directorate General Communication (Brussels: European Commission, 2010).

[6] European Commission, "Special Eurobarometer 359: Attitudes on Data Protection and Electronic Identity in the European Union," ed. Survey coordinated by Directorate-General Communication (Brussels, Belgium: European Commission, 2011).

[7] Sabine Trepte, Tobias Dienlin, and Leonard Reinecke, "Privacy, Self-Disclosure, Social Support, and Social Network Site Use. Research Report of a Three-Year Panel Study, http://opus.uni-hohenheim.de/volltexte/2013/889/pdf/Trepte_Dienlin_Reinecke_2013_Privacy_Self_Disclosure_Social_Support_and_SNS_Use.pdf" (Stuttgart: Universität Hohenheim, 2013).

[8] Susan B. Barnes, "A Privacy Paradox: Social Networking in the Unites States," *First Monday* 11, no. 9 (2006), http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/1394/1312.

[9] Sabine Trepte, Tobias Dienlin, and Leonard Reinecke, "Risky Behaviors: How Online Experiences Influence Privacy Behaviors," in *Von Der Gutenberg-Galaxis Zur Google-Galaxis. From the Gutenberg Galaxy to the Google Galaxy. Surveying Old and New Frontiers after 50 Years of Dgpuk*, ed. Birgit Stark, Oliver Quiring, and Nikolaus Jackob (Wiesbaden: UVK, in press), 217.

[10] Yong J. Park, "Digital Literacy and Privacy Behavior Online," *Communication Research* 40, no. 2 (2013), 217.

on online privacy literacy. Thus, privacy literacy can be understood as an important foundation for deliberation in the field of online privacy debates.[11]

The purpose of this chapter is first to elaborate on the role that privacy literacy plays in explaining internet users' current behaviors and attitudes on privacy. Privacy literacy will primarily refer to data protection knowledge and data protection strategies. It will be shown that privacy literacy might be a stopgap for paradoxical online privacy behaviors. Second, the research on privacy literacy will be reviewed. It will be shown that contemporary conceptualizations lack a universal scope. Consequently, the goal of this chapter is also to provide a comprehensive academic as well as practical understanding of privacy literacy. Third, and at the core of this chapter, the development of the "Online Privacy Literacy Scale" (OPLIS) will be presented. It will be shown that privacy literacy assessment contributes to answering many open questions in research on online privacy. On the basis of a well elaborated privacy literacy assessment, we will be able to better understand whether and how privacy knowledge influences both online behaviors and attitudes with regard to privacy scholarship and policymaking.

14.1.1 Privacy in Online and Offline Contexts

Privacy can be defined as a dynamic process of social boundary management by which individuals grant or deny access to other individuals or one's group.[12,13] *Online privacy* can be referred to as the process of controlling access to the self while using internet services. In an online context, the *desired level of online privacy* defines what kind of privacy and the extent of control over their data users need and want to have. The *achieved level of online privacy* implies the factual privacy that users acknowledge having and executing. Users strive to bring their online privacy in line with their desired level of privacy. They apply behaviors that approximate both their desired and achieved levels of online privacy. The optimization of privacy and self-disclosure is an ongoing and ever-present process that takes place in any kind of conversation. To achieve an optimal level of privacy, users usually either engage in disclosure practices or withdraw from communication with others. Disclosure and withdrawal might be based on either conscious decisions or automatic responses.

[11] Yong J. Park, Scott W. Campbell, and Nojin Kwak, "Affect, Cognition and Reward: Predictors of Privacy Protection Online," *Computers in Human Behavior* 28, no. 3 (2012).

[12] Irwin Altman, *The Environment and Social Behavior*: *Privacy*, *Personal Space*, *Territory*, *Crowding* (Belmont, CA: Wadsworth Publishing Company, 1975).

[13] Alan F. Westin, *Privacy and Freedom* (New York, NY: Atheneum, 1967).

Online contexts, *and social media* in particular, imply certain challenges to managing one's individual privacy.[14] Oftentimes, their affordances contradict privacy expectations.[15] The conflict between privacy behaviors and online behaviors may be reflected in the mirror of online media *functions* and online media *characteristics*.[16,17]

Online media functions: Digital online services allow for and serve the mutual connection of users and the exchange of content. Online services stipulate interactions with either personally known interaction partners[18] or institutions with an economic interest.

Online media characteristics: Online media simultaneously offer services for one-to-one and one-to-many communication or transactions.[19] They can be defined as communication or transaction media for personal communication or mass communication. Communication content and transactions can be exerted by users who are usually known to the person communicating and by transaction or communication partners who are either not consciously addressed (e.g., the wider network of friends) or otherwise unknown. This latter group may include service providers or third parties that have been authorized by service providers or transaction partners (e.g., clients using the users' data for marketing purposes).

It seems that online media *functions* ask for privacy behaviors that are common in private contexts (e.g., talking to friends, buying goods in a warehouse), where the setting and scope of a transaction is more or less set and clear to both partners. However, online media *characteristics* suggest behaviors similar to privacy control in mass media or public contexts. Many online media characteristics (e.g., business practices or number of transaction partners) are unknown to the user and might be untraceable. Based on disparities between online media functions and characteristics, online privacy behaviors seem to be particularly challenging. We assume that the rules and boundary conditions for both online conversations and economic transactions are not as clear to interaction and transaction partners as they are in offline realms. Also, it seems that online communication is largely bound to economic interests that are often not comprehensible to or traceable by users.

[14] Alice E. Marwick and danah boyd, "I Tweet Honestly, I Tweet Passionately: Twitter Users, Context Collapse, and the Imagined Audience," *New Media & Society* 13 (2011).

[15] danah boyd, "Social Network Sites as Networked Publics: Affordances, Dynamics, and Implications," in *A Networked Self*: *Identity*, *Community*, *and Culture on Social Network Sites*, ed. Zizi Papacharissi (New York: Routledge, 2011).

[16] Sabine Trepte, "The Paradoxes of Online Privacy," in Youth 2.0. Connecting, Sharing, and Empowering? Affordances, Uses and Risks of Social Media. edited by Michel Walrave, Koen Ponnet, Ellen Vanderhoven, Jacques Haers en Barbara Segaert.

[17] Trepte, Dienlin, and Reinecke, "Risky Behaviors: How Online Experiences Influence Privacy Behaviors."

[18] Nicole B. Ellison and danah boyd, "Sociality through Social Network Sites," in *The Oxford Handbook of Internet Studies*, ed. William H. Dutton (Oxford: Oxford University Press, 2013).

[19] Jan Schmidt, *Das neue Netz. Merkmale*, *Praktiken und Folgen des Web 2.0* (Konstanz: UVK, 2009).

14.1.2 Privacy Literacy as a Stopgap for the Privacy Paradox

The contrast between offline and online media functions and characteristics makes apparent that the use of online media requires the user to navigate a challenging environment. Consequently, it is not surprising that *online privacy attitudes* often express users' reluctance in terms of online data sharing and other practices of use. In a survey of 26,761 participants from the 27 member states of the European Union, 84 % reported being concerned about the privacy risks that may result from the collection of personal data by internet service providers.[20] Overall, 63 % of Europeans in this study reported having problems disclosing vast amounts of personal data, and 58 % reported that they do not see alternatives to disclosures of this kind.[21] From a longitudinal perspective, it can be stated that these concerns have increased. Whereas in 1970, only 30 % of people interviewed in representative international surveys reported being concerned about privacy issues; in 2000, almost 70 % reported having these concerns.[22] In sum, users seem to be aware of the challenging environments in which they interact.

In contrast to the concerns that have been expressed, users' *online privacy behaviors* paint a different picture. Representative European surveys indicate that 90 % of Europeans disclose their name and address to shop online; 79 % disclose their name to participate in online social networks.[23] Also, self-disclosures in terms of sharing the intimate and often emotional details of one's life have significantly increased in recent years.[24] It has been reported that users are increasingly aware of the importance of using privacy settings on social network sites. However, when it comes to knowledge about which privacy settings they use and why, most users are unaware of their settings.[25,26]

[20] European Commission, "Special Eurobarometer 359: Attitudes on Data Protection and Electronic Identity in the European Union."

[21] Ibid.

[22] Hichang Cho, Jae-Shin Lee, and Siyoung Chung, "Optimistic Bias About Online Privacy Risks: Testing the Moderating Effects of Perceived Controllability and Prior Experience," *Computers in Human Behavior* 26 (2010).

[23] European Commission, "Special Eurobarometer 359: Attitudes on Data Protection and Electronic Identity in the European Union."

[24] Sabine Trepte, Tobias Dienlin, and Leonard Reinecke, "Privacy, Self-Disclosure, Social Support, and Social Network Site Use. Research Report of a Three-Year Panel Study."

[25] Acquisti and Gross, "Awareness, Information Sharing, and Privacy on the Facebook".

[26] Michelle Madejski, Maritza Johnson, and Steven M. Bellovin, "A Study of Privacy Settings Errors in an Online Social Network" (paper presented at the Tenth Annual IEEE International Conference on Pervasive Computing and Communications, Lugano, Switzerland, 2012).

The disparities between online privacy attitudes and online privacy behaviors have previously been termed the *privacy paradox*. Four hypotheses for why these disparities occur have been suggested[27]:

1. The *gratification hypothesis* implies that users weigh the risks and benefits and come to the conclusion that the risks can be justified by the promise of gratification. This conclusion might be based on more or less consolidated decision making. At least three scenarios seem plausible: (a) While weighing the risks and benefits, users might be fully aware of the risks but come to the conclusion that the gratifications that stem from online use—such as social capital or social support—surmount the risks they perceive.[28] (b) Users might over-value the gratifications and underestimate the risks while not being fully aware of the risks they are taking. This scenario has been referred to when considering the online disclosures of young adolescents.[29] (c) In terms of bounded rationality, users might not have all of the information needed or may lack the time or cognitive capacity to draw cognizant conclusions and thus may overestimate the gratifications and underestimate the risks.[30] In all of the scenarios, a tightrope walk takes place between the gratifications on the one hand and the risks on the other.
2. The *measurement bias hypothesis* posits that the privacy paradox is based on biases in the measurement of both privacy attitudes and behaviors. Privacy attitude measures in current research usually refer to abstract menaces and risks such as “data fraud”; however, measures of privacy behavior address individual strategies used to control personal privacy, which is usually applied while using particular online services such as social network sites. It is argued that attitudes and behaviors are unrelated empirically because they are unrelated in the realities of the users.[31] Consequently, behaviors can hardly be expected to be predicted from attitudes.
3. The *social desirability hypothesis* states that users are well aware of the problems that come along with online privacy management due to the large extent of media coverage.[32] Norms, group pressure, and situational constraints might

[27] for an overview cf. Trepte, Dienlin, and Reinecke, “Risky Behaviors: How Online Experiences Influence Privacy Behaviors.”

[28] Nicole B. Ellison et al., “Negotiating Privacy Concerns and Social Capital Needs in a Social Media Environment,” in *Privacy Online. Perspectives on Privacy and Self-Disclosure in the Social Web*, ed. Sabine Trepte and Leonard Reinecke (Berlin: Springer, 2011).

[29] Jochen Peter and Patti M. Valkenburg, “Adolescents’ Online Privacy: Toward a Developmental Perspective,” Ibid.

[30] Herbert A. Simon, “Bounded Rationality and Organizational Learning,” *Organization Science* 2, no. 1 (1991).

[31] Trepte, Dienlin, and Reinecke, “Risky Behaviors: How Online Experiences Influence Privacy Behaviors.”

[32] Ibid.

guide the attitudes reported in surveys. However, users' articulated concerns do not reflect their needs and individual concerns. Consequently, when their behavior is reported, a very different picture might be drawn.

4. The *knowledge gap hypothesis* addresses privacy literacy and holds that people are concerned and would like to behave differently, but their lack of privacy literacy prevents them from reacting in the ways that they think would most adequately reflect their attitudes and needs. Before demonstrating whether and how online privacy literacy could work as a stopgap for the privacy paradox, it will be defined as the following[33]:

Online privacy literacy may be defined as a combination of factual or declarative ("knowing that") and procedural ("knowing how") knowledge about online privacy. In terms of declarative knowledge, online privacy literacy refers to the users' knowledge about technical aspects of online data protection and about laws and directives as well as institutional practices. In terms of procedural knowledge, online privacy literacy refers to the users' ability to apply strategies for individual privacy regulation and data protection.

In the remainder of this chapter, *online privacy knowledge* will be referred to as factual knowledge about online privacy. Factual knowledge questions can usually be answered with "yes" or "no."

Online privacy literacy might be helpful for overcoming disparities between privacy attitudes and behaviors. Previous research has shown that users do not know a lot about online privacy practices, institutions, laws, or strategies. Thus, to further address the privacy paradox, it seems crucial to better understand whether and what users know about privacy literacy. In the following section, we will address previous research on online privacy literacy and how scholars have conceptualized dimensions of privacy literacy.

14.2 The Story so Far: Research on Privacy Literacy

The origins of media literacy research can be traced back to approaches that came from a strategic marketing perspective. We refer to these as the first generation of privacy literacy research. Here, the focus was on consumers' awareness of commercial data collection and use and on their knowledge about potential strategies for protecting their data. In these studies, awareness and knowledge were measured with single items and self-assessments that were made by the respondents. The second generation of privacy literacy scholars addressed internet users' knowledge about the flow of data on the internet. Such studies pointed out that users in general or

[33] For a definition of declarative and procedural knowledge cf. Phillip L. Ackerman, "Knowledge and Cognitive Aging," in *The Handbook of Aging and Cognition*, ed. Fergus I. M. Craik and Timothy A. Salthouse (New York: Psychology Press, 2008).

users of certain websites showed poor knowledge about privacy risks, how websites use their personal data, and how they could control their information. These studies attempted to provide more elaborated measures of objective knowledge about online privacy instead of subjective knowledge and linked users' knowledge to their behavior. Current measures have extended the achievements of these prior generations by accounting for the multidimensionality of online privacy literacy, offering a theoretical foundation, and relating online privacy literacy to central predictors of internet and social media use. The evolution of privacy literacy research will be elaborated in the following. We will point out important prior insights and will present the open questions that we addressed in our current study.

14.2.1 Early Efforts in Conceptualizing Online Privacy Literacy

Already before the rise of social media, scholars addressed knowledge about data collection and use as an important concept for self-determination and effective data protection with regard to direct marketing. Nowak and Phelps[34] specifically focused on consumer knowledge about information control in the context of direct mailing or telemarketing. They referred to unwanted direct mailing or telemarketing calls as symptoms of the inability to control the secondary use of personal information by third parties. The authors subdivided knowledge about information control into three categories: The consumer can have (a) full knowledge of how data are collected and used, (b) knowledge of either how data are collected or how data are used, or (c) no knowledge of collection or use. Although Nowak and Phelps did not empirically examine the objective knowledge of direct marketers' information practices by consumers, their early effort served as a conceptual framework for future surveys and played an important role in pushing empirical research.

Two early empirical studies developed measurements to investigate whether people knew about how to opt out from direct marketing lists.[35,36] Both studies chose a more specific approach by measuring the awareness of one particular data protection strategy. They focused solely on one specific aspect of the broader

[34] Glen J. Nowak and Joseph Phelps, "Direct Marketing and the Use of Individual-Level Consumer Information: Determining How and When Privacy Matters," *Journal of Interactive Marketing* 11, no. 4 (1997).

[35] Mary J. Culnan, "Consumer Awareness of Name Removal Procedures: Implications for Direct Marketing," *Journal of Direct Marketing* 9, no. 2 (1995).

[36] George R. Milne and Andrew J. Rohm, "Consumer Privacy and Name Removal across Direct Marketing Channels: Exploring Opt-in and Opt-out Alternatives," *Journal of Public Policy & Marketing* 19, no. 2 (2000).

concept of privacy literacy. Culnan,[37] for example, investigated how consumers who were aware that they could remove their names from direct mailing lists differed from users who were unaware of this option. She used data from the Harris-Equifax Consumer Privacy Survey 1991, a sample of 1,255 adults representing the population of the continental United States of America. Knowledge was measured with the single item: "Are you aware of any procedures that allow you to remove your name from direct mail lists for catalogues, products and services, or not?" The answer options were "yes," "no," and "not sure." The findings revealed that awareness depended on age, ethnic background, and education. Consumers who were unaware of name removal were, for example, more likely to be younger, less educated, and non-white than those who claimed to know about this option. Despite these interesting findings, the results have to be interpreted with caution because only a single item was used, and participants self-assessed their knowledge. Participants might have overestimated their privacy literacy.

Milne and Rohm[38] were the first to use multiple-choice knowledge items in addition to self-reports to measure people's awareness of direct marketers' data collection practices. The authors argue that privacy can be established only if a consumer is aware of data collection and knowledgeable about name removal mechanisms. In a study of 1,508 randomly selected participants, they measured awareness of data collection with a multiple-choice item asking: "What type of information do you think organizations with which you have done business have about you?" Participants chose from the following options: (a) names and addresses, (b) telephone numbers, (c) credit card information, and (d) purchase history. Indicating three or four answers was classified as being aware of data collection and naming one or two answers as not being aware of data collection. To assess knowledge of name removal mechanisms, participants were asked: "Do you know any ways to remove your name from direct response lists for catalogs, products, and services?" Participants rated their knowledge with "yes," "no," or "I don't know." Only 34 % of the respondents were aware of data collection *and* knew about name removal mechanisms. By distinguishing declarative from procedural knowledge, Milne and Rome introduced two core dimensions of privacy literacy. However, their study was concerned with only one specific context, and their findings relied on participants' subjective assessments. A second generation of scholars addressing online privacy refined existing knowledge scales and identified more dimensions of privacy literacy.

[37] Culnan, "Consumer Awareness of Name Removal Procedures: Implications for Direct Marketing."

[38] Milne and Rohm, "Consumer Privacy and Name Removal across Direct Marketing Channels: Exploring Opt-in and Opt-out Alternatives."

14.2.2 A Second Generation of Research on Privacy Literacy

Extending these early empirical studies, Turow and colleagues,[39,40] conducted two studies to examine consumer knowledge about how websites handle consumer data. In his first study, Turow[41] investigated whether participants ($N = 1{,}200$) agreed with a number of statements with regard to data collection by websites. Participants rated their level of agreement on a 5-point scale ranging from 1 (*strongly agree*) to 5 (*strongly disagree*). The results showed significant uncertainty towards the statements. Only 59 % of the respondents agreed or strongly agreed with the item "When I go to a website, it collects information about me even if I don't register." Fifty-seven percent incorrectly agreed with the item "When a website has a privacy policy, I know that the site will not share my information with other websites or companies." Turow also found that few internet users protect their information: 43 % reported that they block unwanted emails, and 23 % stated that they use software to check for spyware on their computers.

In a second study of 1,500 adolescents who were representative of the US population, Turow, Feldman, and Meltzer[42] demonstrated that the majority of participants (84 %) knew that their online behavior was traceable through cookies and that internet providers track the websites that users have surfed. However, half of the study participants did not know that their demographic data (e.g., home country or city) was passed on to third parties for marketing purposes and that no information with respect to what is done with these data is returned to the service provider or user in exchange for such information. Also, three quarters of the consumers wrongly thought that the mere presence of a privacy policy means that a website will not share their information with other websites or companies. On average, only 7 of 17 statements were answered correctly. The study also showed that participants with higher formal education were able to provide a larger number of correct answers. For example, respondents with a high school diploma were able to answer six statements correctly, whereas respondents with a college degree provided eight correct answers.

[39] Joseph Turow, "Americans and Online Privacy. The System Is Broken. A Report from the Annenberg Public Policy Center of the University of Pennsylvania," (Philadelphia 2003).

[40] Joseph Turow, Lauren Feldman, and Kimberly Meltzer, "Open to Exploitation: America's Shoppers Online and Offline. Report from the Annenberg Public Policy Center of the University of Pennsylvania," in *Annenberg School for Communication Departmental Papers* (*ASC*) (Philadelphia: University of Pennsylvania, 2005).

[41] Turow, "Americans and Online Privacy. The System Is Broken. A Report from the Annenberg Public Policy Center of the University of Pennsylvania."

[42] Turow, Feldman, and Meltzer, "Open to Exploitation: America's Shoppers Online and Offline. Report from the Annenberg Public Policy Center of the University of Pennsylvania."

Both studies[43,44] made an important contribution to the conceptualization of privacy literacy as they elaborated on knowledge about institutional practices and strategies for data protection in the context of telemarketing. As the media environment has changed tremendously in the last 10 years and as users are challenged by technological innovations, privacy literacy is needed in many more ways, especially when using the internet.

Jensen and colleagues[45] designed a meaningful study to investigate knowledge about privacy-relevant technologies. They included a set of knowledge questions with regard to three technologies that potentially pose a risk to users' privacy: cookies,[46] web bugs,[47] and P3P privacy policies.[48] When participants claimed to know these technologies, they had to evaluate their risks and also provide reasons for why these technologies may impact privacy. Participants were given a list of five possible reasons of which only two were correct. The findings showed that there is a strong perception-knowledge discrepancy. For example, 90 % of the sample claimed that they were knowledgeable about the risks that might emanate from cookies, but 85 % of these participants were not able to select at least one correct reason for why cookies might bear risks at all. This combination of self-reported knowledge and objective knowledge testing showed that many users have an inaccurate perception of their knowledge about privacy technologies. Consequently, self-reported data should be scrutinized when privacy literacy is assessed.

As social media—and social network sites in particular—have been gaining in popularity, it has become apparent that internet users are encountering different and manifold environments that require different kinds of skills and knowledge for effectively handling individual online privacy control and data protection. As many people are now using social network sites (e.g., Facebook), online privacy literacy thus evolves and changes according to the dynamic architecture of such platforms. Consequently, some researchers have focused on privacy literacy within specific web applications. Acquisti and Gross[49] surveyed 294 US college students

[43] Turow, "Americans and Online Privacy. The System Is Broken. A Report from the Annenberg Public Policy Center of the University of Pennsylvania."

[44] Turow, Feldman, and Meltzer, "Open to Exploitation: America's Shoppers Online and Offline. Report from the Annenberg Public Policy Center of the University of Pennsylvania."

[45] Carlos Jensen, Colin Potts, and Christian Jensen, "Privacy Practices of Internet Users: Self-Reports Versus Observed Behavior," *Human-Computer Studies* 63 (2005).

[46] Cookies are files on a computer that automatically save information for visited websites so that the websites recognize a user, or store other session or user-related information, when visiting the website repeatedly.

[47] Web bugs – also known as tracking bugs – are tiny, invisible graphics implemented into websites used for statistic web analysis. They capture information about the users of a website like their IP address, visit time, and browser used, and forward this information to a server.

[48] P3P is short for Platform for Privacy Preferences (P3P). It is a technical solution for websites to communicate their privacy policies automatically to users' computers. When visiting a website, user software should be able to immediately evaluate if it meets users' stated privacy preferences.

[49] Acquisti and Gross, "Awareness, Information Sharing, and Privacy on the Facebook".

on their Facebook usage and measured their trust of the network provider and their awareness of their profile visibility settings on the social network site. Their results demonstrated that the majority of the participants claimed to know how to control their profile visibility but that a considerable minority of members were unaware of privacy setting options. For example, 30 % of participants did not know that there is an option to control who can search for and find their profile on Facebook, and 18 % were not aware of the option to control who is able to read the contents of their profile. Moreover, the majority of Facebook users incorrectly believed that Facebook does not collect and combine information about them from various sources (70 %) and that the providers do not share this information with other companies (56 %).

Acquisti and Gross[50] focused on Facebook as a specific application, thus showing that some users are not knowledgeable about privacy control settings within the framework of this specific application and that they have no idea of the data collection practices of the provider. However, internet users today use a variety of different applications such as social network sites, blogs, email providers, online shopping platforms, and online games. Further conceptualizations of online privacy literacy therefore increase the external validity of measurement while referring to different dimensions of the construct.

14.2.3 Current Instruments and Conceptualizations of Online Privacy Literacy

Whereas the insights of the second generation of privacy literacy research have been criticized as being under-theorized, current approaches strive to offer comprehensive conceptualizations as a theoretical groundwork for measurement. Also, state-of-the-art privacy literacy assessments use objective knowledge testing instead of self-assessments. In a study of 975 US-Americans who were interviewed in a telephone survey, Hoofnagle, King, Li, and Turow[51] showed that the majority of participants exhibited a low level of literacy concerning legal online privacy protection. In the survey, they had to decide whether the following statements were true or false: If a website has a privacy policy, it means that (a) the site cannot share information about a user with other companies unless the user gives the website permission, (b) the site cannot give a user's address and purchase history to the government, and (c) the website must delete information it has about a user, such as name and address, if the user requests that they do so. (d) If the providers of a website violate their privacy policy, the user has the right to sue them, and (e) if a company wants to follow a user's internet use across multiple sites on the internet, it must first obtain the permission of the user. All of the five items had to be identified

[50] Ibid.

[51] Chris Hoofnagle et al., "How Different Are Young Adults from Older Adults When It Comes to Information Privacy Attitudes and Policy," (2010).

as "false," but this was done by only 3 % of the participants. Thirty percent did not provide a single correct answer. Adolescents and young adults in particular overestimated legal online privacy protection.

Morrison[52] again contrasted consumers' subjective and objective privacy knowledge. In a study of 825 participants, he measured social network site users' knowledge about data collection and management by organizations. The subjective privacy knowledge scale consisted of the following three items, which had to be rated on a 7-point Likert scale: (a) Compared with most people you know, how would you rate your knowledge about how organizations collect and manage your personal information? (b) In general, I am quite knowledgeable about how organizations collect and manage my personal information; (d) I am quite knowledgeable about how the information I provide to my online social network is collected and managed by companies. Forty-one percent of the participants claimed to have low knowledge (scores between 1 and 3). Only 26 % of the respondents believed they had high knowledge (scores between 5 and 7).

The objective privacy knowledge scale included 10 True/False/Don't know questions based on a privacy quiz posted on the website of the *Office of the Privacy Commissioner of Canada*. Example items were: (a) Organizations can always refuse to supply a product or service if you won't give them permission to collect, use, or disclose your personal information, (b) Under certain circumstances, organizations can disclose their customers' personal information to law enforcement officials without the customers' consent. Contrary to prior findings concerning privacy literacy, the majority of respondents (62 %) passed the test, meaning that at least 50 % of the questions were answered correctly.

Again, the results demonstrated that subjective privacy knowledge differs significantly from objective privacy knowledge. Age and gender were found to play an important role in overconfidence and the underestimation of subjective privacy knowledge: Whereas older (age 55–64) and female respondents underestimated their subjective privacy knowledge, younger and male participants were overconfident. In contrast to subjective privacy knowledge, objective knowledge did not differ by age and gender.

In a recent study, Park[53] specifically addressed and further elaborated on the multidimensionality of online privacy literacy. Park's scale subdivides online privacy literacy into the dimensions: (a) *technical familiarity*, (b) *awareness of institutional surveillance practices*, and (c) *policy understanding*. The first dimension captured familiarity with technical aspects. Respondents have to rate how familiar they are with five items (e.g., HTML, cache, phishing …) on a 6-point scale ranging from 1 (*not at all*) to 6 (*very familiar*). The results of this dimension are thus based on respondents' self-reports. Awareness of institutional surveillance practices addresses knowledge about data tracking by online companies, illegal

[52] Bobbi Morrison, "Do We Know What We Think We Know? An Exploration of Online Social Network Users' Privacy Literacy," *Workplace Review*, no. April 2013 (2013).

[53] Park, "Digital Literacy and Privacy Behavior Online".

use of personal information, and internal data-collection rules. This dimension is investigated with eight true-false items (e.g., A company can tell that you have opened an email even if you do not respond; When you go to a website, it can collect information about you even if you do not *register*). The dimension *policy understanding* is also operationalized with seven true-false items (e.g., Government policy restricts how long websites can keep the information they gather about you; By law, e-commerce sites, such as Amazon, are required to give you the opportunity to see the information they gather about you). Park also measured the frequency with which the respondents engaged in information control behavior. Information control behavior measures daily routines of online information control. Respondents are asked to report the extent to which they are involved in specific information control behaviors on a 6-point scale ranging from 1 (*never*) to 6 (*very often*). Information control behavior is divided into social and technical strategies. The social dimension, which captures active and passive control, consists of eight items (e.g., Have you given a false or inaccurate email address or a fake name to websites because of the privacy concern?). The technical dimension is composed of four items (e.g., Have you cleared your web browser's history?).

The results revealed that higher privacy literacy in any of the three dimensions contributed to frequent engagement in social and technical information control behavior. Park's[54] study supports the notion that higher online privacy literacy has a positive effect on information control behavior. These findings suggest that privacy literacy could serve as a stopgap between privacy attitudes and privacy behavior.

However, knowledge about technical aspects of data protection was measured only via self-reports, and Park did not offer a residual answer such as "I don't know," thus forcing respondents to guess instead of being able to admit that they did not know the answer. By assessing three distinct dimensions of privacy literacy, Park's study extended prior research tremendously. Yet, from a theoretical point of view, online privacy literacy could incorporate even more aspects. Park did not operationalize knowledge about strategies for information control as a dimension of privacy literacy, but rather measured the frequency of participants' information control behavior. However, in a more comprehensive scale for privacy literacy, information control behaviors could be included as an additional literacy dimension: *knowledge about strategies for individual online privacy control*.

14.2.4 Merits and Critical Aspects of Prior Instruments

Prior research has greatly contributed to the understanding of privacy literacy. As privacy generally represents an elusive and complex phenomenon, privacy literacy likewise demands further investigations and methodological considerations. From our reading of the previous work on online privacy literacy, we identified two open questions:

[54] Ibid.

1. *Capturing the multidimensionality of online privacy literacy*: Most online privacy literacy scales have covered only one or two dimensions of privacy literacy.[55] In addition, most attempts to measure privacy literacy have relied on a single item (e.g., familiarity with cookies[56]). Finally, online privacy literacy has often been limited to only one specific application (e.g., Facebook[57]). Consequently, these investigations have not yet fully captured the various dimensions of online privacy literacy.
2. *Self-reports versus objective knowledge*: Previous studies have predominantly relied on self-reports to measure online privacy literacy. Self-assessments, however, might address not only literacy but also self-efficacy—which refers to the anticipation of how individuals think they are able to handle privacy tasks.[58] The evaluation of one's abilities is not always closely related to knowledge.[59] With the exception of some studies,[60,61] differences between subjective and objective privacy knowledge have often remained unconsidered. A comprehensive online privacy literacy scale should consist of objective knowledge questions (declarative knowledge) on the one hand and questions that consider the abilities and strategies of online data protection (procedural knowledge) on the other.

14.2.5 Six Dimensions for an Enhanced Online Privacy Literacy Scale (OPLIS)

On the basis of a literature review of previous online privacy literacy assessment studies (Sects. 14.2.1, 14.2.2, and 14.2.3) and their critical analysis (Sect. 14.2.5), we will present six dimensions of online privacy literacy that we considered for the Online Privacy Literacy Scale (OPLIS).

Dimension 1: *Knowledge about the practices of institutions and online service providers*: In their daily lives, people use a variety of websites, online platforms, and communities that require the disclosure of personal data to provide the user

[55] e.g. Hoofnagle et al., "How Different Are Young Adults from Older Adults When It Comes to Information Privacy Attitudes and Policy."

[56] Milne and Rohm, "Consumer Privacy and Name Removal across Direct Marketing Channels: Exploring Opt-in and Opt-out Alternatives."

[57] Acquisti and Gross, "Awareness, Information Sharing, and Privacy on the Facebook".

[58] Eszter Hargittai, "Survey Measures of Web-Oriented Digital Literacy," *Social Science Computer Review* 23, no. 3 (2005).

[59] Jensen, Potts, and Jensen, "Privacy Practices of Internet Users: Self-Reports Versus Observed Behavior."

[60] e.g. Ibid.

[61] e.g. Morrison, "Do We Know What We Think We Know? An Exploration of Online Social Network Users' Privacy Literacy."

with services. Hence, users need to know how providers handle and use personal data. The first dimension of our online privacy literacy scale thus focuses on knowledge about common practices by institutions and online service providers who collect data from their users. It encompasses a general understanding of the flow of data on the internet and knowledge about implicit rules of data transformation and forwarding through institutions and stakeholders. As Park denotes, “awareness of institutional systems and social practices may well equip individuals to take appropriate actions”.[62] Milne and Rohm[63] already defined awareness of the data collection and processing practices of organizations as indicators of the factual knowledge that is required for online privacy control. Subsequent research has acknowledged that institutional practices are an important dimension of online privacy literacy. Whereas some studies have exclusively investigated internet users’ knowledge about how website providers use data,[64,65,66] others have adopted it as one dimension of a multidimensional construct.[67,68] As personal data can be regarded as a currency that is used to ‘pay’ for a variety of online services, the hows and whys of data use can be considered a crucial dimension of online privacy literacy.

Dimension 2: *Knowledge about the technical aspects of online privacy and data protection*: The second dimension seeks to measure the extent to which people understand the technical side of data protection on the internet. This knowledge has been recognized as an important requirement with regard to effective online data protection and privacy control.[69,70,71] If, for example, users do not know what a firewall is, they presumably are not able to use it correctly. To warrant online privacy, it is particularly important to know about the technical aspects of data protection.

[62] Park, “Digital Literacy and Privacy Behavior Online.”, 217.

[63] Milne and Rohm, “Consumer Privacy and Name Removal across Direct Marketing Channels: Exploring Opt-in and Opt-out Alternatives.”

[64] cf. Turow, “Americans and Online Privacy. The System Is Broken. A Report from the Annenberg Public Policy Center of the University of Pennsylvania.”

[65] cf. Turow, Feldman, and Meltzer, “Open to Exploitation: America’s Shoppers Online and Offline. Report from the Annenberg Public Policy Center of the University of Pennsylvania.”

[66] cf. Hoofnagle et al., “How Different Are Young Adults from Older Adults When It Comes to Information Privacy Attitudes and Policy.”

[67] cf. Morrison, “Do We Know What We Think We Know? An Exploration of Online Social Network Users’ Privacy Literacy.”

[68] cf. Park, “Digital Literacy and Privacy Behavior Online.” p. 2013.

[69] cf. Jensen, Potts, and Jensen, “Privacy Practices of Internet Users: Self-Reports Versus Observed Behavior.”

[70] cf. Amanda Lenhart and Mary Madden, “Teens, Privacy & Online Social Networks. How Teens Manage Their Online Identities and Personal Information in the Age of Myspace,” (Pew Research Center, 2007).

[71] cf. Park, “Digital Literacy and Privacy Behavior Online.”

Dimension 3: *Knowledge about potential privacy threats and risks*: As survey data have shown, only a minority of internet users have experienced privacy invasions, and they tend to attribute higher risks to other users' privacy than to their own.[72] However, being knowledgeable about the potential privacy threats and risks that emerge from different online media is another crucial dimension of deliberate action in online environments. Acknowledging this, for instance, Park[73] implemented one item to measure privacy-specific risk awareness.

Dimension 4: *Knowledge about the laws and legal aspects of data protection in Germany and the European Union*: As prior research has shown, decisive factors for the development and implementation of data protection strategies comprise not only knowledge about technical aspects and institutional practices but also knowledge about privacy policies, laws, and directives.[74,75,76] The understanding of legal regulations is an important prerequisite for users' self-determination in an increasingly complex online world in which the technical possibilities are almost unlimited and institutional practices are becoming less transparent.[77] Only if users know about their personal rights and the legal restrictions placed on commercial institutions can they make informed decisions and control or optimize their privacy in a responsible way.[78] So far, knowledge about privacy policies and data protection laws has been measured by five[79] to seven[80,81] true-false items. The statements about legal regulations chosen by the authors mostly referred to the US or Canada but were formulated in a very general way. As data protection is regulated by country-specific laws and directives, it is important to explicitly highlight which country or region is being referred to while assessing knowledge about laws and directives. The OPLIS takes into account the requirement of country-specific knowledge about data protection regulations. OPLIS focuses on the German legislation and directives of the

[72] Bernhard Debatin et al., "Facebook and Online Privacy: Attitudes, Behaviors, and Unintended Consequences," *Journal of Computer-Mediated Communication* 15 (2009).

[73] Park, "Digital Literacy and Privacy Behavior Online."

[74] Hoofnagle et al., "How Different Are Young Adults from Older Adults When It Comes to Information Privacy Attitudes and Policy."

[75] Park, "Digital Literacy and Privacy Behavior Online."

[76] Joseph Turow, Michael Hennessey, and Amy Bleakley, "Consumers' Understanding of Privacy Rules in the Marketplace," *Journal of consumer affairs* 42, no. 3 (2008).

[77] acatech, *Internet Privacy. Optionas for Adequate Realisation* (*Acatech Study*) (Heidelberg et al.: Springer Verlag 2013, 2013).

[78] Turow, Hennessey, and Bleakley, "Consumers' Understanding of Privacy Rules in the Marketplace."

[79] Hoofnagle et al., "How Different Are Young Adults from Older Adults When It Comes to Information Privacy Attitudes and Policy."

[80] Park, "Digital Literacy and Privacy Behavior Online."

[81] Turow, Hennessey, and Bleakley, "Consumers' Understanding of Privacy Rules in the Marketplace."

European Union. As citizens of the European Union, German internet users benefit from the harmonization of data protection regulations across EU member states. Hence, knowledge of EU directives on privacy and data protection is also relevant to German internet users as data processing on the internet is not limited to national borders.

Dimension 5: *Knowledge about strategies for individual online privacy control*: Besides knowing about institutional practices and potential privacy threats as well as about technical and legal aspects of data protection and online privacy, the user has to be able to take specific measures and to apply specific strategies of data protection when using the internet. As knowledge about strategies for individual online privacy control is closely linked to the other dimensions of online privacy literacy,[82] it can be seen as a dimension that combines several aspects of technical and legal knowledge as well as knowledge about institutional practices. Unlike those aforementioned dimensions, this dimension captures procedural knowledge. As such it can be defined as "the ability to control the acquisition and use of personal information",[83] including a combination of social (e.g., reduce the online disclosure of personal information to a minimum) and technical skills (e.g., clearing the web browser's cache). Although prior research has already highlighted the importance of procedural knowledge about individual privacy regulation strategies,[84,85,86,87] there has been no appropriate multidimensional scale to measure literacy in data protection strategies.

Dimension 6: *Knowledge about ways to deal with privacy threats*: With this dimension, we aimed to capture a more specific kind of procedural knowledge. Dimension 5 focuses on regulation strategies that are part of a user's everyday internet routine and may be understood as the user's response to the practices of web service providers. It is thus closely linked to factual knowledge about institutional practices and technical aspects of online privacy (Dimensions 1 and 2). By contrast, procedural *knowledge about ways to deal with privacy threats* is based on knowledge about potential privacy threats and risks and the legal regulations of online privacy (Dimensions 3 and 4). Internet users

[82] Park, "Digital Literacy and Privacy Behavior Online."

[83] Milne and Rohm, "Consumer Privacy and Name Removal across Direct Marketing Channels: Exploring Opt-in and Opt-out Alternatives.", 239.

[84] Culnan, "Consumer Awareness of Name Removal Procedures: Implications for Direct Marketing."

[85] Milne and Rohm, "Consumer Privacy and Name Removal across Direct Marketing Channels: Exploring Opt-in and Opt-out Alternatives."

[86] Morrison, "Do We Know What We Think We Know? An Exploration of Online Social Network Users' Privacy Literacy."

[87] Park, "Digital Literacy and Privacy Behavior Online."

have to be able to identify a privacy threat and they have to be familiar with online privacy control to effectively proceed against the offender. We suggest this dimension because it measures whether internet users know what to do in case of an emergency, how to avoid online privacy violations, and how to retrieve their online privacy in case of a current violation.

14.3 Towards the Online Privacy Literacy Scale (OPLIS)

Three aims were pursued for the development of the OPLIS: First, the design of the scale was based on previous research and on the attempt to gain a comprehensive understanding of how online privacy literacy can be defined. Second, the scale was designed to cover all relevant dimensions of online privacy literacy and different forms of media use. Third, it investigates literacy with either multiple-choice test questions or true-false items. Whereas the former format offers benefits by reducing the guessing probability to 25 %, the latter format is simple and economical with regard to processing and analysis.[88] The answer option "I don't know" was offered with both formats to reduce the likelihood of guessing.[89]

We took three steps to pursue these aims. First, an extensive analysis of the literature was conducted to identify the most important dimensions of privacy literacy (cf. Sect. 14.2). Second, these dimensions were tested and extended through a content analysis (cf. Sect. 14.3). From the content analysis, relevant fragments had to be identified for all of the dimensions and worded as knowledge items (examples from each dimension will be given in Sect. 14.3.2). Third, the item pool generated by the content analysis must be tested with representative surveys to establish the validity and reliability of the items and scales. This third step is still a work in progress.

14.3.1 Design of the Content Analysis

To gain a broad understanding of privacy literacy, we conducted a qualitative content analysis of various documents and sources related to data protection and online privacy. This approach was chosen because it is particularly suited for the reduction of complexity and the comprehension of information. It furthermore provides the

[88] Lee A. Clark and David Watson, "Constructing Validity: Basic Issues in Objective Scale Development," *Psychological Assessment* 7, no. 3 (1995).

[89] Morrison, "Do We Know What We Think We Know? An Exploration of Online Social Network Users' Privacy Literacy."

possibility of continuously reviewing and adapting the categorical system.[90] This is particularly important as we wanted to keep our categorical system open to the addition of new dimensions of privacy literacy. The method seemed most appropriate for gaining maximal expertise on the subject and furthermore to create an item pool that would cover all aspects that might be relevant for online privacy literacy.[91]

14.3.1.1 Categories

We used a coarse categorical framework consisting of the six privacy literacy dimensions that were identified in prior research (cf. Sect. 14.2.5 of this chapter).

In line with the reconstructive method by Gläser and Laudel,[92] the categorical system was kept open to ensure the possibility of adding new dimensions and categories while extracting content. Moreover, using a pretest, several subcategories for each dimension were defined to structure the coding procedure.

14.3.1.2 Selection of Relevant Literature and Documents

The sample for the content analysis consisted of text documents from five different sources that captured a broad spectrum of privacy topics. In the following, we will refer to why and how the sample was drawn from all five sources.

First, a full sample of *scientific journal articles focusing on privacy literacy and privacy knowledge* was included in the sample. By taking into account all relevant prior research on privacy literacy, previous findings could be incorporated into the scale. References in the data bases *Academic Search Premier*, *PsycARTICLES*, and *PsycINFO* were searched for the keywords "privacy literacy", "privacy knowledge", and "digital literacy". As a second selection criterion, we checked the abstracts of the references we obtained and selected articles that theoretically or empirically addressed online privacy literacy.

Second, *project deliverables* were included. We considered project reports of interdisciplinary research projects dealing with privacy in digital environments. Legal data protection, institutional practices, consumer needs, as well as behaviors concerning privacy and data protection have been summarized in these project deliverables. They can be considered rich sources for generating factual and procedural knowledge items. All of the current projects funded by the European Union and the German National Academy of Science and Engineering (acatech) that are related to privacy were taken into account.

[90] Jochen Gläser and Grit Laudel, *Experteninterviews und qualitative Inhaltsanalyse als Instrumente rekonstruierender Untersuchungen*, 4th ed. (Wiesbaden: VS Verlag, 2010).

[91] Clark and Watson, "Constructing Validity: Basic Issues in Objective Scale Development."

[92] Gläser and Laudel, *Experteninterviews und qualitative Inhaltsanalyse als Instrumente rekonstruierender Untersuchungen.*

Third, a sample of *news and magazine articles* was drawn with the aim of gaining insight into what users should know about online privacy and data protection. The mass media often report on issues and public debates concerning online privacy and data collection and these reports may be more up-to-date than other sources. The sample period was from November 2012 to October 2013. Circulation was used as a first selection criterion and search keywords as a second. We selected two high-quality German newspapers with the widest circulation, *Süddeutsche Zeitung* and *Frankfurter Allgemeine Zeitung*, and two high-circulation magazines specializing in computers and IT: *ComputerBild* and *c't magazine*. The media content was accessed via online data bases (*Frankfurter Allgemeine Archiv*, *Süddeutsche Zeitung Archiv*, *WISO*). The keywords "online privacy" and "online data protection" were used to search the data bases to find relevant articles.

Fourth, *EU directives on privacy and data protection*, *the German constitution*, *and laws concerning online privacy and data protection* were sampled. They build the legal framework for the online privacy of German internet users. The EU directives *1995/46/EC on data protection*, *1997/66/EC on privacy in the telecommunication sector*, *2000/31/EC on electronic commerce*, *2002/58/EC on electronic communication*, *2006/24/EC on data retention*, and the E*U regulation 2001/45/EC on the processing of personal data* as well as relevant articles of the *Charter of fundamental rights of the EU* were included. German legislative texts that were included were: *Federal Data Protection Act* (*BDSG*), *Telecommunications Act* (*TKG*), *Telemedia Act* (*TMG*), *Copyright Law* (*UrhG*, *KunstUrhG*), *decisions of the Federal Constitutional Court* (*BVerG*), and relevant articles from the *German Constitution* (*GG*). The contents of all relevant directives and legislative texts could thus be considered for analysis.

Fifth, we analyzed the contents of current *privacy policies of major online service providers* for factual knowledge about institutional practices as well as for procedural knowledge about users' opportunities to control their privacy. We defined five categories of online service providers: E-commerce platforms, online banking providers, search engines, email providers, and social media. For each category, the privacy policies of the providers with the widest coverage in Germany were selected for analysis. For an overview of the selected documents, see Table 14.1.

In all, 395 documents comprised the sample for the content analysis. Forty-five percent of these documents were articles from computer magazines (*ComputerBild* and *c't magazine*), and 38 % were news articles. Six coders went through all of the documents identifying text passages that contained information relevant for any of the a priori defined dimensions of privacy literacy or privacy literacy in general. In the latter case, they defined a new category in which they coded the identified text passage. The general selection criterion was formulated as a question: "Do internet users need to know this information (described in the document) in order to be capable of regulating their online privacy?"

Table 14.1 Documents selected for the content analysis

Scientific literature (full sample)
Journal articles focusing on "privacy literacy"
Project deliverables (full sample)
Acatech (2012, 2013), Eurobarometer (2010, 2011), PRISMS (2013), SurPRISE (2013)
Legislative texts (full sample, effective October 2013)
Germany (BDSG, GG, TKG, TMG, UrhG, KunstUrhG, decisions of the BVerG)
European Union (EU directives 1995/46/EC, 1997/66/EC, 2000/31/EC, 2002/58/EC, 2006/24/EC, EU regulation 2001/45/EC on processing of personal data, Charter of fundamental rights of the EU)
Privacy policies of major online service providers (Retrieved on the 30th of October 2013)
E-commerce platforms (Amazon, Ebay)
Online banking provider (Sparkasse)
Search engines (Google, Yahoo)
Email provider (GMX, WEB, Googlemail)
Social media (Facebook, Wordpress, XING)
News articles[a] (November 1st 2012 to October 31st 2013)
FAZ – Frankfurter Allgemeine Zeitung
Süddeutsche Zeitung
Computer magazine articles[b] (November 1st 2012 to October 31st 2013)
ComputerBild
c't magazine

[a] *FAZ* and *Süddeutsche Zeitung* are nationwide newspapers that have more than one million readers per issue. We chose to analyze these daily newspapers as they have the highest coverage in Germany. Institut für Demoskopie Allensbach, "Awa 2013 – Allensbacher Marktanalyse und Werbeträgeranalyse," (2013), http://www.ifd-allensbach.de/fileadmin/AWA/AWA2013/Codebuchausschnitte/AWA_2013_BandMedien_Basistabelle.pdf

[b] In order to gain more information about current strategies and to integrate specialized knowledge from computer and data-protection experts, two computer magazines were included in the sample. Whereas *ComputerBild* has the highest coverage in Germany among computer magazines, the *c't magazine* represents a more specialized magazine that is read by computer scientists and experts

14.3.2 Results

In total, 2,597 extracts resulted from the content analysis. They were coded according to the predefined and continuously adapted and modified categorical system, whereby most extracts were assigned to the dimension *knowledge about the practices of organizations*, *institutions*, *and online service providers* (819 extracts) and *knowledge about the laws and legal aspects of data protection* (643 extracts). In a subsequent step, doubles and irrelevant extracts were identified. The dimensions *knowledge about potential privacy threats and risks* and *knowledge about ways to deal with privacy threats* were dismissed because the remaining dimensions already contained most of the information that could have been coded into these categories. Five dimensions of privacy literacy were confirmed by the content analysis: (1) *Knowledge about the practices of organizations*, *institutions*, *and* *online service providers*; (2) *knowledge about the technical aspects of online privacy and data protection*; (3) *knowledge about the laws and legal aspects of online data protection in Germany*; (4) *knowledge about European directives on privacy and data protection*; and (5) *knowledge about user strategies for individual online privacy control.*

In an iterative process, the remaining extracts were transformed into multiple-choice test questions or true-false items (each with the residual answer "*I don't know*"). The resulting item pool was comprised of approximately 25 items in each dimension and 113 in total. In the following, each dimension will be described in detail.

14.3.2.1 Dimension 1: Knowledge About the Practices of Organizations, Institutions, and Online Service Providers

Extracts falling into this dimension included common online practices such as data surveillance, data collection, data processing, data analysis, data transmission, and data deletion by authorities and internet companies such as social media (e.g., *Facebook*, *Twitter*, *Google+*), search engine providers (e.g., *Google*, *Yahoo*, *Bing*), online banking providers and providers of e-commerce platforms (e.g., *Amazon*, *Ebay*), but also governments and intelligence agencies. In the EU project deliverable *SurPRISE*,[93] for example, the following extract was coded:

> In Germany, the surveillance of email communication has increased significantly since 2009. In 2010, German intelligence services inspected 37,292,862 emails and data connections, a number quintupled from 2009, when 6.8 million Internet and other network communications were inspected. Over 15,300 key words related to the topics of terrorism, proliferation, immigrant smuggling and trafficking were used to filter emails, but only led to actually useful clues in 213 investigation cases.

Specifically, the privacy policies of companies such as *Facebook* have revealed a number of common data collection and data mining practices. Knowing the contents of privacy policies hence becomes an important aspect of this dimension. An extract from *Facebook*'*s* privacy policy, for example, indicates precisely what such companies do with their users' data:

> We receive data if you visit a website that has a social plugin. We store these data for a period of 90 days. Afterwards, we delete your name and other identity-related information or combine them with data from other people in such a way that these data cannot be linked to your person.[94]

[93] SurPRISE, "Surveillance, Privacy and Security: A Large Scale Participatory Assessment of Criteria and Factors Determining Acceptability and Acceptance of Security Technologies in Europe - D 3.1 – Report on Surveillance Technology and Privacy Enhancing Design," (2013).

[94] Original extract (in German): "*Wir erhalten Daten, wenn du eine Webseite mit einem sozialen Plug-In besuchst. Wir speichern diese Daten für einen Zeitraum von bis zu 90 Tagen. Danach entfernen wir deinen Namen sowie alle anderen personenbezogenen Informationen von den Daten*

Table 14.2 Example Items for Dimension 1

Example items of the dimension "*knowledge about the practices of organizations, institutions, and online service providers*"	
Companies are able to provide users with online advertising that is based on their surfing behavior.	True
Social network sites (e.g., Facebook) collect and analyze user data.	True
Companies are able to detect whether someone has opened an email even if the receiver does not reply.	True

Other extracts revealed the infrastructure and data flow in companies such as *Google*. In the following example, it can be seen that knowledge about institutional practices also means a greater understanding of the data flow and the architecture of the internet:

> Google processes personal data on our servers, which are located in various countries around the world. Thus, we might process your data on a server that is not located in your country.[95]

These short extracts from different documents were then transformed into knowledge items. Although more than 100 items were generated from the extracts in this dimension, the final item pool contained 22 items (Table 14.2).

14.3.2.2 Dimension 2: Knowledge About Technical Aspects with Regard to Online Privacy and Data Protection

The content analysis revealed that there were a number of technical solutions for online privacy and online data protection. Thus, the examples primarily revealed technical solutions for data protection with regard to hardware (e.g., router, intranets) and software (e.g., firewalls, data encryption, antispyware, specific browser settings and features such as cache and browsing history). Furthermore, the dimension also included examples explaining the technical infrastructure or functionality of the web (e.g., HTML, IP addresses, and Cloud Computing). A smaller number of extracts addressed knowledge about the technical processes of data stealing (e.g., phishing through Trojans or other malware) and techniques for data tracking.

It was noticeable that many documents focused on data encryption when discussing privacy-enhancing technologies (PETs). In *c't magazine*, which specializes in computer technologies in particular, the following text passage was extracted:

oder kombinieren sie mit den Daten anderer Personen auf eine Weise, wodurch diese Daten nicht mehr mit dir verknüpft sind." (Facebook, Privacy Policy; Retrieved on the 30th of October 2013)

[95] Original extract (in German): "*Google verarbeitet personenbezogene Daten auf unseren Servern, die sich in zahlreichen Ländern auf der ganzen Welt befinden. Daher verarbeiten wir Ihre personenbezogenen Daten gegebenenfalls auf einem Server, der sich außerhalb des Landes befindet, in dem Sie leben.*" (Google, Privacy Policy; Retrieved on the 30th of October 2013)

Table 14.3 Example Items for Dimension 2

Example items of the dimension "***knowledge about the technical aspects of online privacy and data protection***"	
What is a Trojan? A computer program that...	(a) ... **is disguised as a useful application but covertly and secretly executes other functions in the background**
	(b) ... protects the computer from viruses and other malware
	(c) ... was invented only for fun and does not have a specific function
	(d) ... caused damage as a computer virus in the 90s but does not exist anymore
All browsers automatically support the current Transport Layer Security (TLS 1.2)	False
Companies are able to detect whether someone has opened an e-mail even if the receiver does not reply	True

> In the end, only the server defines which type of encryption will be used. Although the browser can express preferences, large servers in particular tend to ignore this and use the encryption type that is most appropriate for them from the list specified within the browser.[96]

Another example extract that focused on malware and how it affects users' privacy was found in the EU deliverable *SurPRISE*:

> The Trojan is usually brought onto the device covertly. This can occur in different ways: for example, the visit to a prepared website link (drive-by download) or the opening of an e-mail attachment may trigger the installation. Other possibilities are the usage of so-called infection proxies or direct physical access to the device.[97]

All in all, 54 items were created from these extracts, 28 items of which were retained for the final item pool (Table 14.3).

14.3.2.3 Dimension 3: Knowledge About the Laws and Legal Aspects of Online Data Protection in Germany

The last two dimensions comprise examples of German laws and directives from the European Union concerning online data protection. We coded fundamental rights in the German constitution, especially the right to informational self-determination and

[96] Original extract (in German): "*Letztlich entscheidet immer der Server, welches Verschlüsselungsverfahren zum Einsatz kommt. Der Browser kann zwar Präferenzen äußern, aber insbesondere größere Server ignorieren die in der Regel und nehmen stattdessen das aus der Liste des Browsers, was sie für angemessen halten*" (c't magazine, vol. 18, 2013, p. 16).

[97] SurPRISE, "Surveillance, Privacy and Security: A Large Scale Participatory Assessment of Criteria and Factors Determining Acceptability and Acceptance of Security Technologies in Europe - D 3.1 – Report on Surveillance Technology and Privacy Enhancing Design."

Table 14.4 Example Items for Dimension 3

Example items for the dimension “*knowledge about the laws and legal aspects of online data protection in Germany*”	
All providers of social network sites in Germany have to apply the same privacy policy. Deviations have to be indicated	False
German law prohibits the spreading of abusive or incorrect information about a person on one’s own profile or the profile of the concerned person on a social network site	True
By German law, when are online service providers allowed to use and analyze personal data for personalized advertising?	(a) Always
	(b) **If the user has consented to it**
	(c) If the purpose of it is noncommercial
	(d) Never
	(e) Don’t know

applicable German laws concerning data protection conditions. As data protection is not just the responsibility of the individual, it became apparent that a user has to know his or her rights concerning online data transmission. The following passage was extracted from the *acatech* project deliverable:

> The principle of data minimization (not contained in EU law, but in § 3a BDSg) demands that data collection should be kept to a minimum with regard to conducted business and data processing systems should be built in a data minimizing manner.[98]

The extracts were consequently transformed into 51 multiple-choice and True/False/Don’t know questions. Twenty-three items concerning German laws on data protection were retained in the final item pool (Table 14.4).

14.3.2.4 Dimension 4: Knowledge About European Directives on Privacy and Data Protection (Table 14.5)

As Germany is part of the European Union, a German internet user might also refer to EU regulations, general directives, and special directives on data retention and the processing of personal data, all of which have to be implemented into national law by EU member states. Extracts from this dimension included all decisions about data protection that have been specified in these directives. An example passage extracted from *Regulation* (*EC*) *No 45/2001* would be:

> Personal data shall only be processed for purposes other than those for which they have been collected if the change of purpose is expressly permitted by the internal rules of the Community institution or body.

[98] acatech, *Internet Privacy. Options for Adequate Realisation* (*Acatech Study*).

Table 14.5 Example Items for Dimension 4

Example items of the dimension "*knowledge about European directives on privacy and data protection*"	
Directives of the European Union concerning data protection . . .	(a) . . . count as transnational data protection laws
	(b) . . . **have to be implemented into national data protection laws by EU member states**
	(c) . . . serve only as guidelines for national data protection laws
	(d) . . . do not exist yet
	(e) Don't know
By European law, it is legal to forward anonymous data for market research	True
Directives of the European Union prohibit the processing of data that reflect racial or ethnic background, political opinions, and religious or philosophical beliefs without explicit consent	True

A total of 56 items concerning European law were created from which 16 items were included in the final item pool.

14.3.2.5 Dimension 5: Knowledge About User Strategies for Individual Online Privacy Control

In this dimension, example extracts indicated strategies that help to ensure online privacy and data protection. In contrast to knowledge about technical aspects or institutional practices, knowledge about strategies is characterized as knowing how to protect data by passive or active actions. *Passive actions* incorporate control strategies such as the nondisclosure of personal information or opting out of services that require the disclosure of personal data. An example extract is:

> Hiding can be effective if a person communicates anonymously. Yet, hiding can also refer to not disclosing information about age, gender, or location.[99]

Active actions include the use of encryption software, privacy-enhancing technologies, antispyware and privacy-related browser settings support data protection (e.g., clearing the web browser history and deleting the cache and cookies). In the

[99] Original extract (in German): "*Verbergen kann vollständig sein, zum Beispiel wenn anonym kommuniziert wird. Verbergen kann sich aber auch nur auf bestimmte Aspekte beziehen wie zum Beispiel Alter, Geschlecht oder Aufenthaltsort.*" *acatech, Privatheit Im Internet. Chancen Wahrnehmen, Risiken Einschätzen, Vertrauen Gestalten (Acatech Position) (Heidelberg u.a.: Springer Verlag 2013, 2013).*

Table 14.6 Example Items for Dimension 5

Example items of the dimension *“knowledge about strategies for individual online privacy control”*	
In order to protect one’s privacy, it is useful to regularly delete the browsing history, the cache, and saved cookies	True
It is safe to use one secure password that consists of upper and lowercase letters, numbers, and special characters for all online accounts and profiles	False
Not disclosing any information online is not a good strategy for protecting data and privacy	False

magazine *ComputerBild*, the following strategy was proposed for guaranteeing more security online (Table 14.6):

> No one can attack a wireless network that has been switched off. If you go on vacation, unplug the wireless network or deactivate it. Also activate the “night option” of your router so that it switches off your wireless network at night.[100]

All in all, 37 items were generated of which 22 items were included in the final item pool.

14.4 Discussion

With the research presented in this chapter, we aimed at developing a reliable and valid scale for measuring online privacy literacy. Privacy literacy has often been identified as a possible solution for overcoming the disparities of users’ privacy attitudes and behaviors. Also, an ongoing assessment of citizens’ privacy literacy might help to provide an online-privacy-behavior evaluation that can be used for policy, legal, and educational purposes.

In a methodological sense, a new and comprehensive scale for privacy literacy is needed because prior studies have not covered all aspects and dimensions that may be relevant to online privacy literacy.[101,102,103,104] On the basis of our argumentation,

[100] Original extract (in German): “*Ein ausgeschaltetes WLAN kann niemand angreifen. Wenn Sie verreisen, drücken Sie den WLAN-Schalter, deaktivieren die Funktion im Menü oder ziehen den Stromstecker. Stellen Sie den Router unter System und Nachtschaltung so ein, dass er WLAN nachts generell abschaltet*.” (ComputerBild, vol. 15, 2013, p. 68).

[101] Hoofnagle et al., “How Different Are Young Adults from Older Adults When It Comes to Information Privacy Attitudes and Policy.”

[102] Morrison, “Do We Know What We Think We Know? An Exploration of Online Social Network Users’ Privacy Literacy.”

[103] Turow, “Americans and Online Privacy. The System Is Broken. A Report from the Annenberg Public Policy Center of the University of Pennsylvania.”

[104] Turow, Feldman, and Meltzer, “Open to Exploitation: America’s Shoppers Online and Offline. Report from the Annenberg Public Policy Center of the University of Pennsylvania.”

we believe that privacy literacy is not unidimensional but consists of diverse aspects of factual and procedural knowledge. Furthermore, previous studies have been based on self-reported measures of privacy literacy.[105,106,107] But as Morrison demonstrated, subjective assessments of knowledge do not necessarily correspond with objective knowledge.[108] With the development of the OPLIS, we tried to address both points of criticism. As a multidimensional scale, the OPLIS covers five distinct dimensions of online privacy literacy. Furthermore, all five dimensions will be presented as a knowledge test. The scale includes both multiple-choice items and true-false items to permit an objective assessment of online privacy literacy.

14.4.1 Limitations

By using a qualitative, in-depth content analysis to achieve a broad and comprehensive understanding of privacy literacy, we aimed to cover the multidimensional structure and various aspects related to online privacy literacy. Nonetheless, a number of limitations have to be taken into account. First, the institutional practices and data protection strategies identified through the content analysis reflect a general awareness and refer to regulation strategies that can be mapped onto many online situations. It is important to acknowledge that using specific applications requires additional literacy within the framework of this application. We plan on developing media-specific subscales to address the individual characteristics of different online applications in the future.

A second limitation is related to knowledge about the legal aspects of online data protection. So far, only German and EU laws concerning data protection and online privacy have been incorporated. This limitation refers to only two of the five dimensions. We have plans to extend the item pool to address international law and country-specific legal regulations.

Third, online privacy and data protection happens in a dynamic and changing environment. The internet is driven by innovations, new technologies, and applications that require users to constantly learn about new ways of data flow and new strategies for online privacy control. A reliable scale for measuring privacy literacy thus requires a regular review and further development to ensure that it is topical and up-to-date.

[105] Culnan, "Consumer Awareness of Name Removal Procedures: Implications for Direct Marketing."

[106] Milne and Rohm, "Consumer Privacy and Name Removal across Direct Marketing Channels: Exploring Opt-in and Opt-out Alternatives."

[107] Park, "Digital Literacy and Privacy Behavior Online."

[108] Morrison, "Do We Know What We Think We Know? An Exploration of Online Social Network Users' Privacy Literacy."

14.5 Conclusion and Outlook

In the present chapter, we argued that online privacy literacy could serve as a stopgap between privacy attitudes and privacy behavior. It has been widely assumed that people who are concerned about their privacy want to behave accordingly but that lacking privacy literacy prevents them from effectively regulating their online privacy. A lack of knowledge about individual online privacy control strategies, legal and technical aspects, as well as institutional practices might hence provide one explanation for why users' behavior on the internet seems paradoxical. Looking at results from prior research, the case is quite alarming: Internet users do not know how to protect their personal data or how to regulate their individual privacy efficiently; also, information about business practices and the laws and regulations affecting privacy is scarce.[109,110]

The item pool that we created with a content analysis was tested in a convenience sample to identify difficult items.[111] In a second step, the remaining pool of items was tested in a sample that is representative of the German population.[112] Scale reliability, discriminant and convergent validity, as well as item difficulties were analyzed.

Accordingly, with the OPLIS, future research on online privacy will have a comprehensive instrument for measuring privacy literacy. It will enable scholars and policy makers alike to precisely measure how much people know about protecting their personal data and controlling their individual privacy. That being said, in many discussions—particularly with regard to the use of mass media but also in other fields such as health communication, security, or politics—literacy and knowledge are viewed as a universal remedy in crisis situations or in settings in which consumer behaviors do not match political or societal expectations. Political and educational systems are invited to provide literacy to those who do not behave or act according to social norms. With regard to privacy in the modern digital world, we find ourselves in a crisis as previous understandings of privacy are largely undermined by online practices. Yet, we have to ask if we can actually help users and contribute to a better 'online world' by suggesting knowledge and literacy enhancements as a solution. Isn't online privacy literacy a paternalistic argument that adheres to standards of privacy that may seem obsolete to users? We do not have answers to any of these questions. Thus, for us as researchers, online privacy research—not only on privacy literacy but also on what people want, do, and need—is an ongoing challenge and task we would like to commit to.

[109] Hoofnagle et al., "How Different Are Young Adults from Older Adults When It Comes to Information Privacy Attitudes and Policy."

[110] Turow, Feldman, and Meltzer, "Open to Exploitation: America's Shoppers Online and Offline. Report from the Annenberg Public Policy Center of the University of Pennsylvania."

[111] Sabine Trepte, Philipp K. Masur, and Doris Teutsch "Measuring Internet Users' Online Privacy Literacy. Development and Validation of the Online Privacy Literacy Scale (OPLIS)," (in prep).

[112] Ibid.

References

acatech. *Internet Privacy. Options for Adequate Realisation (Acatech Study)*. Heidelberg et al.: Springer Verlag, 2013.

acatech. *Privatheit Im Internet. Chancen wahrnehmen, risiken einschätzen, Vertrauen gestalten (Acatech Position)*. Heidelberg u.a.: Springer Verlag, 2013.

Ackerman, Phillip L. "Knowledge and Cognitive Aging." Chap. 9 In The Handbook of Aging and Cognition, edited by F. I. M. Craik and T. A. Salthouse, 445–89. New York: Psychology Press, 2008.

Acquisti, Alessandro, and Ralph Gross. "Awareness, Information Sharing, and Privacy on the Facebook." Paper presented at the 6th Workshop on privacy enhancing technologies, June 28 – June 30 2006, Cambridge, June 2006.

Altman, Irwin. *The Environment and Social Behavior: Privacy, Personal Space, Territory, Crowding*. Belmont, CA: Wadsworth Publishing Company, 1975.

Barnes, Susan B. "A Privacy Paradox: Social Networking in the Unites States." *First Monday* 11, no. 9 (2006). http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/1394/1312.

boyd, danah. "Social Network Sites as Networked Publics: Affordances, Dynamics, and Implications." In A Networked Self: Identity, Community, and Culture on Social Network Sites, edited by Zizi Papacharissi, 39–58. New York: Routledge, 2011.

Cho, Hichang, Jae-Shin Lee, and Siyoung Chung. "Optimistic Bias About Online Privacy Risks: Testing the Moderating Effects of Perceived Controllability and Prior Experience." *Computers in Human Behavior* 26 (2010): 987–95.

Clark, Lee A., and David Watson. "Constructing Validity: Basic Issues in Objective Scale Development." *Psychological Assessment* 7, no. 3 (1995): 309–19.

Culnan, Mary J. "Consumer Awareness of Name Removal Procedures: Implications for Direct Marketing." *Journal of Direct Marketing* 9, no. 2 (1995): 10–19.

Debatin, Bernhard, Jennette P. Lovejoy, Ann-Kathrin Horn, and Brittany N. Hughes. "Facebook and Online Privacy: Attitudes, Behaviors, and Unintended Consequences." *Journal of Computer-Mediated Communication* 15 (2009): 83–108.

Ellison, Nicole B., and danah boyd. "Sociality through Social Network Sites." In *The Oxford Handbook of Internet Studies.*, edited by W. H. Dutton. Oxford: Oxford University Press, 2013.

Ellison, Nicole B., Jessica Vitak, Charles Steinfield, Rebecca Gray, and Cliff Lampe. "Negotiating Privacy Concerns and Social Capital Needs in a Social Media Environment." Chap. 3 In *Privacy Online. Perspectives on Privacy and Self-Disclosure in the Social Web*, edited by Sabine Trepte and Leonard Reinecke, 19–32. Berlin: Springer, 2011.

Eurobarometer. "E-Communications Household Survey." edited by Directorate General Communication. Brussels: European Commission, 2010.

European Commission. "Special Eurobarometer 359: Attitudes on Data Protection and Electronic Identity in the European Union." edited by Survey coordinated by Directorate-General Communication. Brussels, Belgium: European Commission, 2011.

Gläser, Jochen, and Grit Laudel. *Experteninterviews und Qualitative Inhaltsanalyse als Instrumente rekonstruierender Untersuchungen* [in German]. 4th ed. Wiesbaden: VS Verlag, 2010.

Hargittai, Eszter "Survey Measures of Web-Oriented Digital Literacy." *Social Science Computer Review* 23, no. 3 (2005): 371–79.

Hoofnagle, Chris J., Jennifer King, Su Li, and Joseph Turow. "How Different Are Young Adults from Older Adults When It Comes to Information Privacy Attitudes and Policy." 2010.

Institut für Demoskopie Allensbach. "Awa 2013 – Allensbacher Marktanalyse Und Werbeträgeranalyse." (2013). http://www.ifd-allensbach.de/fileadmin/AWA/AWA2013/Codebuchausschnitte/AWA_2013_BandMedien_Basistabelle.pdf.

Jensen, Carlos, Colin Potts, and Christian Jensen. "Privacy Practices of Internet Users: Self-Reports Versus Observed Behavior." *Human-Computer Studies* 63 (2005): 203–27.

Lenhart, Amanda, and Mary Madden. “Teens, Privacy & Online Social Networks. How Teens Manage Their Online Identities and Personal Information in the Age of Myspace.” Pew Research Center, 2007.

Madejski, Michelle, Maritza Johnson, and Steven M. Bellovin. “A Study of Privacy Settings Errors in an Online Social Network.” Paper presented at the Tenth Annual IEEE International Conference on Pervasive Computing and Communications, Lugano, Switzerland, 2012.

Marwick, Alice E., and danah boyd. “I Tweet Honestly, I Tweet Passionately: Twitter Users, Context Collapse, and the Imagined Audience.” New Media & Society 13 (2011): 114–33.

Milne, George R., and Andrew J. Rohm. “Consumer Privacy and Name Removal across Direct Marketing Channels: Exploring Opt-in and Opt-out Alternatives.” *Journal of Public Policy & Marketing* 19, no. 2 (2000): 238–49.

Morrison, Bobbi. “Do We Know What We Think We Know? An Exploration of Online Social Network Users’ Privacy Literacy.” *Workplace Review*, no. April 2013 (2013): 58–79.

Nowak, Glen J., and Joseph Phelps. “Direct Marketing and the Use of Individual-Level Consumer Information: Determining How and When Privacy Matters.” *Journal of Interactive Marketing* 11, no. 4 (1997): 94–108.

Park, Yong J. “Digital Literacy and Privacy Behavior Online.” *Communication Research* 40, no. 2 (2013): 215–36.

Park, Yong J., Scott W. Campbell, and Nojin Kwak. “Affect, Cognition and Reward: Predictors of Privacy Protection Online.” *Computers in Human Behavior* 28, no. 3 (May 2012): 1019–27.

Peter, Jochen, and Patti M. Valkenburg. “Adolescents’ Online Privacy: Toward a Developmental Perspective.” Chap. 16 In *Privacy Online. Perspectives on Privacy and Self-Disclosure in the Social Web*, edited by Sabine Trepte and Leonard Reinecke, 221–34. Berlin: Springer, 2011.

Schmidt, Jan. *Das Neue Netz. Merkmale, Praktiken und Folgen des Web 2.0*. Konstanz: UVK, 2009.

Simon, Herbert A. “Bounded Rationality and Organizational Learning.” *Organization Science* 2, no. 1 (1991): 125–34.

SurPRISE. “Surveillance, Privacy and Security: A Large Scale Participatory Assessment of Criteria and Factors Determining Acceptability and Acceptance of Security Technologies in Europe – D 3.1 – Report on Surveillance Technology and Privacy Enhancing Design.” 2013.

Taddei, Stefano, and Bastianina Contena. “Privacy, Trust and Control: Which Relationships with Online Self-Disclosure?” *Computers in Human Behavior* 29, no. 3 (2013): 821–26.

Trepte, Sabine “The Paradoxes of Online Privacy.” Youth 2.0. Connecting, Sharing, and Empowering? Affordances, Uses and Risks of Social Media, edited by Michel Walrave, Koen Ponnet, Ellen Vanderhoven, Jacques Haers en Barbara Segaert.

Trepte, Sabine, Tobias Dienlin, and Leonard Reinecke. “Privacy, Self-Disclosure, Social Support, and Social Network Site Use. Research Report of a Three-Year Panel Study.” Stuttgart: Universität Hohenheim, 2013. http://opus.uni-hohenheim.de/volltexte/2013/889/pdf/Trepte_Dienlin_Reinecke_2013_Privacy_Self_Disclosure_Social_Support_and_SNS_Use.pdf.

Trepte, Sabine, Tobias Dienlin, and Leonard Reinecke. “Risky Behaviors: How Online Experiences Influence Privacy Behaviors.” In *Von Der Gutenberg-Galaxis Zur Google-Galaxis. From the Gutenberg Galaxy to the Google Galaxy. Surveying Old and New Frontiers after 50 Years of DGPuK*, edited by B. Stark, O. Quiring and N. Jackob. Wiesbaden: UVK, 2014.

Trepte, Sabine, and Leonard Reinecke. “The Social Web as Shelter for Privacy and Authentic Living.” Chap. 6 In *Privacy Online. Perspectives on Privacy and Self-Disclosure in the Social Web*, edited by Sabine Trepte and Leonard Reinecke, 61–74. Berlin: Springer, 2011.

Trepte, Sabine, Philipp K. Masur, and Doris Teutsch. “Measuring Internet Users’ Online Privacy Literacy. Development and Validation of the Online Privacy Literacy Scale (OPLIS).” in prep.

Tufekci, Zeynep. “Can You See Me Now? Audience and Disclosure Regulation in Online Social Network Sites.” *Bulletin of Science, Technology & Society* 28, no. 1 (2008): 20–36.

Turow, Joseph. “Americans and Online Privacy. The System Is Broken. A Report from the Annenberg Public Policy Center of the University of Pennsylvania.” Philadelphia, 2003.

Turow, Joseph, Lauren Feldman, and Kimberly Meltzer. “Open to Exploitation: America’s Shoppers Online and Offline. Report from the Annenberg Public Policy Center of the University of Pennsylvania.” In *Annenberg School for Communication Departmental Papers (ASC)*. Philadelphia: University of Pennsylvania, 2005.

Turow, Joseph, Michael Hennessey, and Amy Bleakley. “Consumers’ Understanding of Privacy Rules in the Marketplace.” *Journal of consumer affairs* 42, no. 3 (2008): 411–24.

Westin, Alan F. *Privacy and Freedom*. New York, NY: Atheneum, 1967.

Chapter 15
LEAP: The LEAP Encryption Access Project

Elijah Sparrow and Harry Halpin

Abstract As demonstrated by the recent revelations of Edward Snowden on the extent of pervasive surveillance, one pressing danger is in the vast centralization of unencrypted messages by centralized silos such as Microsoft, Facebook, and Google. Peer-to-peer alternatives for messaging have failed to reach massive uptake amongst users. In response, we argue for a client-service federated model of messaging service providers that provide automatic encryption of messages such as email. We then present the threat model and design of LEAP, which currently provisions opportunistic email encryption combined with a VPN and cross-device synchronization. We also outline how the next steps for LEAP could allow massive deployment of mix networks and be extended to new services such as chat, file-sharing, and social networking.

Keywords Usability • Cryptography • Encryption • VPN • Federation

15.1 Introduction

Why in the era of mass surveillance is encrypted email still nearly impossible? Take for example the case of the journalist Glenn Greenwald, who could not properly set-up encrypted email when Edward Snowden contacted him to leak the NSA secrets. Despite Snowden personally creating a video tutorial for Greenwald, the journalist still had difficulty installing the software and understanding how encryption worked, causing him to nearly lose the chance to tell the story of the NSA's pervasive surveillance to the world. In fact, a friend had to mail Greenwald USB thumb-drives with the software for encrypted e-mail and chat pre-installed for Greenwald to use the software (Greenwald 2014).

E. Sparrow (✉)
LEAP Encryption Access Project, PO Box 4422, Seattle, WA 98194, USA
e-mail: elijah@leap.se

H. Halpin
W3C/MIT, 32 Vassar Street, Room 32-G515, Cambridge, MA 02139, USA
e-mail: hhalpin@w3.org

S. Gutwirth et al. (eds.), *Reforming European Data Protection Law*,
Law, Governance and Technology Series 20, DOI 10.1007/978-94-017-9385-8_15

This lack of progress in over three decades in securing email via encryption and privacy-preserving techniques is precisely what allows both content and metadata analysis of email by agencies such as the NSA to be pervasive and nearly inescapable. Even well-understood technologies such as OpenPGP-based e-mail encryption are not used by the vast majority of people for reasons that have been understood for nearly a decade and a half (Whitten and Tygar 1999). While there has been considerable progress in the deployment of IP-address level anonymity via the Tor project, most people rely on insecure and centralized silos for e-mail. This is a tremendously dangerous situation: We consider the *right to whisper*, the ability to exercise freedom of speech without surveillance, to be a central and necessary precondition for a free society. As advances in surveillance technology have rapidly eroded this right, the lack of secure communication threatens to become a true threat to core freedoms in both repressive contexts and liberal democracies.

There are few working solutions for encrypted and anonymous e-mail. While Tor provides the best solution for IP-level anonymity, this is defeated when users rely on centralized e-mail systems where the dangers of their communication being intercepted via disclosures by the server are considerable (Dingledine et al. 2004). For example, many users simply use Tor to "anonymize" their access to email services such as Gmail that can simply hand over their data, or even systems such as *riseup.net* that likely have all outgoing and ingoing traffic monitored even if the server itself refuses requests for user data. Beyond e-mail, Off-the-Record messaging for chat works well, but requires synchronous chat between two users.[1] Other attempts to deploy censorship-resistant messaging applications have been within a peer-to-peer (P2P) framework, such as Tribler (Pouwelse et al. 2008).[2] Despite the hype, these peer-to-peer systems have not been adopted by almost any users. One common way for existing users to encrypt e-mail messages is via using Thunderbird with the Enigmail plug-in, yet users find it difficult to use as all key management is manual.[3] Current high-profile efforts such as Mailpile are aimed at essentially replacing the user-experience of Thunderbird and Enigmail, not at actually solving the underlying problems of key management and provisioning encrypted e-mail.[4] Our goal should be mass adoption of encrypted e-mail. To achieve mass adoption of encrypted e-mail, key provisioning and managing the server-side must be done as well as an excellent client-side user experience. This lack of usable tools for even basic tasks such as message authentication or digital signatures has led to an acceptance of poor security across the globe, even among civil society actors who urgently need the ability to communicate safely. Yet when

[1] http://www.cypherpunks.ca/otr/

[2] Although Tribler itself does not use encryption or anonymization techniques, but instead seems to mistakenly uphold that a peer-to-peer architecture is enough to be resistant to censorship threats.

[3] http://www.enigmail.net/home/index.php

[4] http://mailpile.is

users attempt to secure their communications, they face confusing software, a dearth of secure providers, and a greater risk of being flagged as potential troublemakers. In other words, problems of usability, availability, and adoption.

Our solution to this problem is called LEAP, a recursive acronym for the "LEAP Encryption Access Project." LEAP is still in development, although the core functionality of basic opportunistic encryption email is now available for beta testing.[5] An OpenVPN client and key management via techniques described herein (in particular, Soledad and Nicknym) are complete. Of course, work on new methods of key discovery and validation is ongoing, and the work on mix networking aspects has yet to begin but is outlined in terms of architecture. Once basic services are provided such as email, other services are planned to be deployed in the following order: chat, file storage, VoIP, social networking (status updates), and distributed document editing. We believe the current LEAP client and platform architecture presented below, although currently only working for e-mail, can be scaled to chat and other federated services easily while maintaining the advantages of LEAP-assisted encryption as regards usability and security. Once this solid foundation has been laid and there has been significant uptake of e-mail, tools not currently supported by various silos (advanced decision-making, alternative crypto-currencies) may even be investigated. At this point the most important task is wide review of the core concepts and open-source code. The LEAP system's client and server are open-source and non-profit, and we hope will lead to a network of surveillance resistant e-mail providers emerging to help tackle pervasive surveillance. The project source-code on Github is available to all.[6]

In response to this state of affairs, in Sect. 15.2 we argue for a federated model of decentralized servers that provision services such as encrypted email to many user clients. We claim a 'server-assisted' architecture can have numerous deployment and privacy advantages if designed correctly. In Sect. 15.3 we discuss the threat model that we need to defeat with a new overall design. In Sect. 15.4, we present the design of LEAP in detail and in Sect. 15.5 demonstrate how this general model successfully does opportunistic email encryption. Lastly in section "Future Research and Conclusion", we outline how the next steps for the LEAP system may preserve user anonymity against even global passive adversaries using mix networking and discuss future work to extend to new services such as chat, file-sharing, and social networking.[7]

[5] To try, follow instructions on http://demo.bitmask.net

[6] https://github.com/leapcode/

[7] Note that parts of Sects. 15.2 and 15.4 are modified versions of material available on the LEAP wiki at http://leap.se/en/docs (Accessed May 23rd 2014).

15.2 Landscape of Secure Architectures

First, a few words on terminology: In general, we will consider the application layer of services that a user wants to use as a messaging system for natural language between users on top of the network (IP) level. These applications are exemplified by email, status updates, chat, or even VoIP rather than file-sharing or web-browsing. The social graph of the user is the identity of which user communicates to which other users.

Every messaging architecture makes certain design choices that privilege one property over another. Although there may be no intrinsic trade-offs between different security properties such as authenticity and functional properties such as usability, the architecture of actual implementations are structurally biased toward certain properties and against others. In general, there are three broad types of systems: *peer-to-peer*, where each sender can communicate autonomously to any other receiver without any mediating parties, centralized *silos* where every sender (client) must to go through a single organization (the silo) to communicate to a receiver (who must in turn receive the message via the same silo), and *federated* systems where every sender has to go through at least one server to communicate to a receiver, but the sender and receiver may be on different servers operated by distinct organizations. Examples of silos for messaging would include Facebook and Twitter, while federated systems include Jabber chat and email. Gmail and Microsoft Live would technically be federated systems as they are based on e-mail, but they attempt to replicate the silo model as much as possible by centralizing as many users on a single server as possible. There are no widely deployed peer-to-peer messaging systems, but BitTorrent would be a good example of a widely deployed peer-to-peer system for file-sharing. While virtually unused, Tribler would be an example of the use of a peer-to-peer architecture for messaging (Pouwelse et al. 2008).

Each of these architectures has a number of security and functional properties: availability (ability for messages to be sent and received in a timely manner), usability (ease of use by user), authenticity (authentication of user identity), control (can the user move to a different server or client), anonymity (can system be used without a personal identification), and unmappability (inability to detect the user's social graph). Many of these architectures do not use encryption (Twitter, Facebook, Tribler, e-mail) but we are interested in those that do, such as peer-to-peer architectures including GNUNet,[8] silos such as the first version of Cryptocat[9] and Mega's proposed encrypted service[10] (as well as the systems deployed by Silent Circle[11] and Lavabit,[12] and federated systems such as OpenPGP email[13]

[8] https://gnunet.org/

[9] https://crypto.cat/

[10] https://mega.co.nz/

[11] https://silentcircle.com/

[12] https://lavabit.com/

[13] http://www.openpgp.org/

Table 15.1 Security and functional properties comparison per architecture

Property	P2P	Silo	Federated
Availability	Low	High	High
Usability	Low	High	Low
Control	High	Low	High
Authenticity	High	Low	High
Anonymity	Low	Low	Low
Unmappability	Low	Low	Low

as implemented by plug-ins such as Enigmail and Jabber with Off-the-Record messaging). In Table 15.1, we can see the trade-offs of each these architectures in very broad terms.[14] Note that the use of terms 'low' and 'high' are relative, and relatively better is not necessarily good. For example, federated and peer-to-peer models have better authenticity than silo models, but usability problems make it so that their authenticity is often poor in practice.

In contrast to a silo such as Facebook that runs continuously with high availability, in peer-to-peer systems an available low latency path to another peer can not be guaranteed. This also holds for federated systems, although less so as the number of servers is relatively low so path latency tends to be higher. Furthermore, peer-to-peer systems tend to fail to be usable, requiring special software be installed, as do many federated systems. User control tends to be low in silos, as users usually cannot retrieve their data and can by definition only communicate to other users of the silo, unlike peer-to-peer and federated systems. Authenticity tends to be high in peer-to-peer systems as peers can authenticate to peers, but can remain anonymous insofar as they do not have to authenticate to any master server unlike in silos and federated systems. In practice, the authenticity of peer-to-peer systems is often low, since many users do not properly use shared secrets or check key fingerprints. However, all systems fail to be unmappable. Silos by nature maintain all personal data in a centralized form accessible to system administrators, while federated systems fragment this between multiple servers. Even federated and peer-to-peer systems that allow anonymous usage reveal the social graph of their users to outside adversaries rather easily via traffic analysis, which is perhaps the one saving virtue of silos: At least with a silo, an outside adversary can't determine your friends. The information gained by mapping a social graph of any given user can usually reveal their identity even if a system allows users to join a communication channel without revealing their anonymity.[15]

Unfortunately, these problems with the properties above appear to be unsolved regardless of which architectural approach a user takes (centralized authority, distributed peer-to-peer, or federated servers). Indeed, in this regard the federated

[14] Note that we do understand reasonable people may disagree over the exact values, and furthermore, that we are describing only a class of deployed systems rather than particular hypothetical systems or systems that do not have mass deployment.

[15] For example, monitoring the patterns of communication in an IRC channel that allows anonymous identifiers can eventually reveal the identities of users of the IRC channel.

approach does not actually solve all the problems of secure communication perfectly, but rather is a deployment strategy with certain security properties that allow it to fight the disadvantages of the peer-to-peer approach (sybil attacks and latency) and the centralized silo approach (single point of failure). If a centralized system only has to communicate with itself, it can solve the hard problems by trusting itself completely and thus only communicating within its trust boundary. However, this is unrealistic for many cases such as chat or email, and still contains the fatal flaw of a single point of failure. It is possible to safely ignore many of these problems if a system also ignores usability or matching the features that users have grown accustomed to with contemporary methods of online communication. Yet if a new system does care about usability and features, then it will demonstrate value across all these properties and so tackle any contingent problems in implementation.

15.3 Threat Model and Design

We consider the primary goal of stopping pervasive surveillance making it technically as difficult as possible for the contents of a message to be read by any party other than the intended recipient while preserving as much as possible the privacy of both sender and recipient. What is a necessary first step is end-to-end encryption applied to the actual content of messages from client to client. For our threat model, we are considering two distinct types of attack, an *active server attacker* that focuses decrypting messages on the server and a *global passive adversary* that simply copies all messages (encrypted or not). For attackers, the goal is to gain access to the content of the encrypted messages and to determine the social graph of who is communicating to whom. For decrypting messages, attacking a single server with many clients makes more sense than attacking many clients for most attackers. For this section, we will consider only the first attacker, as the second is more difficult to solve and an area for future research (see section "Future Research and Conclusion").

The active server attacker uses either technical attacks or legal means to force a server to hand over the private keys of its users so the attacker can decrypt the encrypted messages. To prevent this, the private key material must not remain on any server, so that an attacker cannot decrypt the encrypted message by compromising the server or placing the server under compulsion. A case in point would be Lavabit, which had a single point of failure by virtue of being a company incorporated in the United States, so legal compulsion forced its shutdown.

How can we keep a federated model while the keeping the keys on the client? The problem can be broken down into a number of distinct components: server-side infrastructure, usable client software, and the fundamental protocol itself. Current OpenPGP-compliant or other content encryption protocols are difficult to set-up for many end-users and server administrators. As a result only a few large servers such as Google or activist e-mail servers under considerable threat (such as *riseup.net*) implement the server-side infrastructure for the protocols such as proper use of DKIM,[16] and while standards like S/MIME[17] are more widely supported, they are ignored by webmail clients and even many non-Web clients. LEAP facilitates such infrastructure deployment by creating "puppet" (automation) scripts for many of the harder tasks involved in setting-up a privacy-enhanced and secure email provider.[18] Yet setting up certificate pinning[19] and other best practices for email service providers is not enough. What is necessary is to have the client and server actively work together in order to encrypt the message, so to prevent the situation where private key materials are stored only on the server and defended only by weak defenses such as passwords.

Simply storing the private key on a single device of the user, as done by most encrypted mail programs, is not enough as users now want to read their e-mail through multiple devices. The main problem facing such a system is safely getting the correct keys onto users devices. LEAP accomplishes this through a multipurpose client that appears to the user simply as an OpenVPN[20] client, which is more accurately called the "Encrypted Internet Proxy" (EIP) client in LEAP (as different transport protocols could be used, such as Tor, rather than OpenVPN). However, there is more than meets the eye to the EIP functionality in the LEAP client: The LEAP client is bundled with the routines for generating, validating, and discovering keys as well as synchronizing keys and related material (such as the status of messages being "read" across multiple devices). This is the heart of the LEAP system.

Key storage and operations in the LEAP client piggyback on an OpenVPN EIP client since many users who would not install a native email reader application such as Thunderbird due to their preference for Web-based mail, but users likely would install a VPN on their system to enable activities such as file-downloading or watching streaming videos, but would not install an obtuse program just to aid key management. The LEAP client can then also generate keys, and with the help of the server can even manage the keys by using server-enabled discovery and trusted validation of public keys for the recipient of an email. Lastly, while some email clients such as Mailpile may natively supports encryption, LEAP allows users to continue using their existing non-Web e-mail client by providing a local SMTP proxy that captures unencrypted email, encrypts it, and then sent it out using the LEAP protocols.

[16] http://www.dkim.org/

[17] http://tools.ietf.org/html/rfc5751

[18] http://docs.puppetlabs.com/guides/introduction.html

[19] https://tools.ietf.org/html/draft-perrin-tls-tack-02

[20] http://openvpn.net/

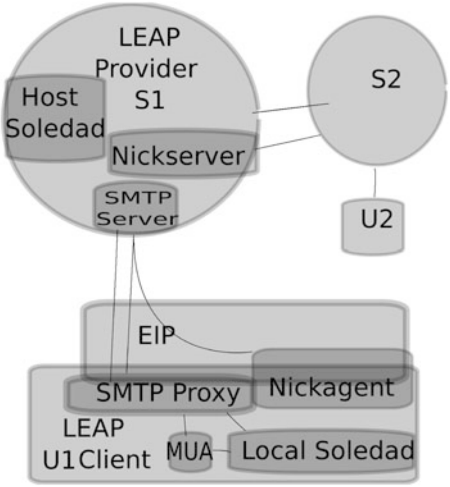


Fig. 15.1 Components of LEAP email architecture

15.4 State of LEAP Client-Server Architecture

The LEAP architecture consists of two main components, the *LEAP Platform* and the *LEAP Client*. Illustrated in Fig. 15.1, we show how a single server (S_1) runs the LEAP Platform that is accessed by a user (U_1) with a LEAP client installed on their machine, so that LEAP-enabled server can then encrypt messages to another server (S_2) so they may reach another user (U_2). Note that the user U_2 may be connected to another LEAP-enabled server or may simply be using public key encryption technologies of their choice, such as Thunderbird or Outlook.

The LEAP platform offers a set of automation tools to allow an organization to deploy and manage a complete infrastructure for providing user communication services. The LEAP client is an application that runs on the user's local device and is tightly bound to the server components of the LEAP Platform. The client is auto-updating (via Tor's Thandy[21]), auto-configuring, and cross platform. Although message security rests entirely on a foundation of authenticity, since without proper validation of encryption keys a user cannot be assured of confidentiality or integrity, current systems of establishing message authenticity are so difficult to use that many users simply ignore this step (Gaw et al. 2006). LEAP will address authenticity by not only having opportunistic encryption but also strong and automatic identity validation. Lastly, recent advances in social network analysis have made unmappability an urgent requirement for any architecture that seeks to address the surveillance situation, which LEAP plans to address with graph resistant routing. Improvement in these areas will come at a price: Although LEAP

[21] https://git.torproject.org/checkout/thandy/master/

communication tools will be backward compatible with existing federated standards such as SMTP, a user of the LEAP system will not have the same degree of choice in client software and providers as does a user of a traditional federated system.

15.4.1 LEAP Platform

The LEAP Platform consists of a command line tool and a set of complementary puppet modules. The recipes allow an organization to operate one or more clusters of servers to provision LEAP-enabled services. With the LEAP command line tool, a system administrator can rapidly deploy a large number of servers, each automatically configured with the proper daemons, firewall, encrypted tunnels, and certificates.

The LEAP Platform recipes define an abstract service provider, with recipes for complementary services that are closely integrated together. To create an actual infrastructure, a system administrator creates a "provider instance" by creating simple configuration files in a filesystem directory, one for each server. Typically, a system administrator will not need to modify the LEAP Platform recipes, although they are free to fork and merge as desired. The "provider instance" directory tree should be tracked using source control and is a self-contained encapsulation of everything about an organization's server infrastructure (except for actual user data).

15.4.2 LEAP Data Storage

One design goal of the LEAP platform is for a service provider to act as a "untrusted cloud" where data are encrypted by the client before being sent to the server and we push as much of the communication logic to the client as possible. There are a few cases where the server must have knowledge about a user's information, such as when resolving email aliases or when processing support requests. In the current implementation, data storage is handled by BigCouch, a distributed document-centric database server.[22] Every user has a personal database for storing client encrypted documents, like email and chat messages. Additionally, there are several non-encrypted databases containing the minimal information needed to connect user accounts to optional support tickets and even billing details. The LEAP Platform includes a web application for user and administrator access to these non-encrypted databases, although future research will hopefully be able to minimize if not eliminate this information.

[22] http://bigcouch.cloudant.com/

15.4.3 Soledad

Soledad ("Synchronization Of Locally Encrypted Data Among Devices") is responsible for client-encrypting user data, keeping it in sync with the copy on the server and a user's other devices, and for providing local applications with a simple API for document storage, indexing, and search. Soledad is implemented on the LEAP client to store email messages, the user's public and private OpenPGP keys, and a contact database of validated public keys.

Soledad is based on U1DB, but modified to support encryption of both the local database replica and every document before it is synchronized with the server.[23] Local database encryption is provided by a block-encrypted SQLite database[24] via SQLCipher.[25] Documents synchronized with the server are individually block encrypted using a key derived produced via an HMAC of the unique document id and a long storage secret. In order to prevent the server from sending forged or old documents, each document record stored on the server includes an additional client-computed MAC derived from the document id, the document revision number, and the encrypted content. The server time-stamps each update of the database, so that Soledad's MAC and HMAC key used to encrypt the client database can only send the server new databases. The key for every device is attached to LEAP client.

15.4.4 Nicknym

One of the main features of the LEAP system is to provide strong authentication of public keys in a way that is easy for users. To do this, LEAP relies on a newly implemented protocol called Nicknym. Simply put, Nicknym maps user nicknames to public keys. With Nicknym, the user is able to think solely in terms of nicknames, while still being able to communicate with a high degree of security (confidentiality, integrity, and authenticity). Essentially, Nicknym is a system for binding human-memorable nicknames to a cryptographic key via automatic discovery and automatic validation. When a new name is found that is not in a Nicknym database, Nicknym can fall back to legacy methods such as HKP (HTTP Keyserver Protocol) and the X.509 infrastructure when necessary, using the result of any keys found inquiring on a public key server.[26] However, these legacy methods often are not very secure and reveal valuable traffic-based information, but we nonetheless believe finding a public key for a user is in general worth it, even if cannot be done in a completely bullet-proof manner. The LEAP client thus prefers LEAP-validated keys that do not expose the keys of users unnecessarily.

[23] https://one.ubuntu.com/developer/data/u1db/

[24] https://sqlite.org/

[25] http://sqlcipher.net/

[26] https://tools.ietf.org/html/draft-shaw-openpgp-hkp-00

Nicknym is a federated protocol: A Nicknym address is in the form *username@domain* (just alike an email address). Like LEAP as a whole, Nicknym includes both a client and a server component. Although the client can fall back to legacy methods of key discovery when needed, domains that run the Nicknym server component enjoy much stronger identity guarantees. Existing forms of cryptographic identity pose a serious problem for people who value their security. These systems rely on either a single trusted entity (e.g. Skype), a vulnerable X.509 Certificate Authority system (e.g. S/MIME), or key identifiers that are difficult to use and not human memorable (e.g. OpenPGP, OTR). Because a user cannot ensure confidentiality or integrity without confirming the authenticity of the other party, authenticating public keys remains a bedrock precondition for any message security. Nicknym is a protocol to solve this problem in a way that is backward compatible, easy for the user, and includes strong authenticity.

Nicknym attempts to solve the binding problem by using methods LEAP calls "provider keys" and "federated web of trust" (FWOT) between providers, although checking them requires the user to begin with an initial contact. The X.509 and HKP infrastructure can be used to look for keys. In all cases, the LEAP provider can check for provider keys to help counter attacks on TOFU[27] provided a record of the keys in question are kept in a LEAP Platform-accessible key registry. Network perspectives can work to ensure the honesty of all LEAP providers in providing both their provider keys and the keys for their users.

Nicknym starts with TOFU of user keys, because it is easy to do and backward compatible with legacy providers. In TOFU, a client naively accept the key of another user when it first encounters it. When a user accepts a key via TOFU, the user is making a bet that possible attackers against the user did not have the foresight to specifically target the user with a false key during discovery. Of course, this would not be true with an active adversary, and so the use of provider keys (with a federated web-of-trust) is to used to prevent these kinds of attacks.

Next, we add checks against the X.509 infrastructure (including HKP), which may be available using popular key servers. For those providers that publish the public keys of their users, we require that these keys be fetched over validated TLS. This makes third party attacks against TOFU more difficult, but also places a lot of trust in the providers (and certificate authorities).

Then, we check for provider keys. If a service provider supports Nicknym, the public keys of its users are additionally signed by a "provider key." If a LEAP client has the correct provider key, a user sending a message via a provider no longer need to TOFU the keys of the provider's users. This has the benefit making it possible for a user to issue new keys, and to add support for very short-lived keys rather than trying to use key revocation. A service provider is much less likely to lose their private key or have it compromised, a significant problem with TOFU of user keys.

Finally, we add a Federated Web of Trust (FWOT). The system works like this: Each service provider is responsible for the due diligence of properly signing the

[27] TOFU stands for "Trust On First Use," which assumes the first transfer and use of a key is not compromised.

keys of a few other providers, akin to the distributed web of trust model of OpenPGP, but with all the hard work of proper signature validation placed upon the service provider. When a user communicates with another party who happens to use a service provider that participates in the FWOT, the user's client will automatically trace a chain of signature from the other party's key, to their service provider, and then to the user's own service provider (with some possible intermediary signatures). This allows for identity that is verified through an end-to-end trust path from any user to any other user in a way that can be automated and is human memorable. Support for a FWOT allows LEAP to bypass entirely X.509 Certificate Authorities, to gracefully handle short lived provider keys, and to handle emergency re-key events if a provider's key is lost. As one moves down this list, each measure taken gets more complicated, requires more provider cooperation, and provides less additional benefit than the one before it. Nevertheless, each measure contributes some important benefit toward the goal of automatic binding of an user identity to public key.

To ameliorate the case where a provider provides false keys, we add a simple form of network perspectives where the client can ask one provider what key another provider is distributing. This allows a user's client to be able to audit their provider and keep them honest in an automated manner. If a service provider distributes bogus keys, their users and other providers will be quickly alerted to the problem.

The problem with Nicknym's mix of methods is that these methods could conflict with one another. For instance, if TOFU was overrun by providers signing new user keys, a provider could create a new key for a user, and override any trust on first use and perspectives for a short time by just announcing a new key – and one could even imagine the provider can easily switch the keys back to reduce the chance of being caught by the user. However, these methods compliment each other to avoid this conflict. When establishing trust the steps are taken in linear order, with that order reversed to maintain trust. If the server was malicious, network perspectives and a federated web of trust could catch the change of keys. LEAP would not want to prevent providers from publishing signed keys, as that trust anchor is required to revoke and update keys. In the case where malfeasance is detected, the network of LEAP-enabled providers will be alerted to the exception, and ultimately a social investigation into the cause of the problem must be done.

15.4.5 LEAP Client

The *LEAP client* is an application that runs on a user's own device and is responsible for all encryption of user data, and includes currently the following components: *Encrypted Internet Proxy* (OpenVPN), *Soledad* (multi-device user data synchronization), *Key Manager* (Nicknym agent and contact database), and *email proxy* (opportunistic email encryption). The client must be installed a user's device before they can access any LEAP services (except for user support via the web application). Written in Python (with QT, OpenVPN, SQLcipher), the LEAP client currently runs across Linux, Windows, and Mac operating systems.[28] When a user installs a LEAP client, a *first-run* wizard walks the user through the simple process of authenticating or registering a new account with the LEAP provider of their choice (using Secure Remote Password[29] so that the server never sees a cleartext copy of the password).

The client is auto-updating, using Tor's Thandy library to update library dependencies as needed. Unlike other update systems, Thandy updates are controlled by a timestamp file that is signed each day. This ensures that the client will not miss an important update and cannot be pushed an old or compromised update by an attacker.

15.4.6 Encrypted Internet Proxy

The goal with LEAP's Encrypted Internet Proxy (EIP) service is to provide an automatic, always on, trouble-free way to encrypt a user's network traffic. The EIP service encrypts all of a user's traffic, is auto-configuring, and works hard to prevent data leakage from DNS, IPv6, and other common client misconfigurations that are not tackled by OpenVPN. Currently OpenVPN is used for the transport (OpenVPN uses TLS for session negotiation and IPSec for data encryption). OpenVPN was selected because it is fast, open source, and cross-platform. In the future, LEAP plans to add support for Tor as an alternate transport. EIP is more than OpenVPN, but also a key manager that is necessary in order to place a public-private keypair on the user's device to let them add new devices and synchronize them with Soledad (as described in Sect. 15.4.3).

When started, the LEAP client discovers the service provider's proxy gateways, fetches a short-lived X.509 client certificate from the provider if necessary, and probes the network to attempt to connect. If there are problems connecting, the LEAP client will try different protocol and port combinations to bypass common ISP firewall settings since VPN access is typically blocked crudely by simple port and protocol rules, not deep packet inspection.

By default, when a user starts the computer the next time, client will auto-connect the EIP. The client will display the status of the EIP in the task tray (Windows, Linux), menu bar (Mac), or notification drawer (Android). The user interface is very limited, principally restricted to connecting, disconnecting, and troubleshooting. If disconnected while the proxy is active, the LEAP client will automatically attempt to reconnect when the network is again available.

[28] An Android version, with has considerable differences due to being coded in Java, is under development.

[29] https://tools.ietf.org/html/rfc5054

15.5 LEAP in Action: Opportunistic Email Encryption

The LEAP email service is designed to client encrypt messages whenever possible, be compatible with existing mail user agents, provide strong authentication of recipient public keys, allow communication with existing email providers, and be as user friendly as possible. Additionally, when mail is relayed to other LEAP providers, the LEAP platform will automatically establish and require opportunistic encryption for the SMTP transport, adding a layer of forward secrecy to encrypted email (so long as neither service provider is compromised).

For incoming email, messages are received by the service provider's MX servers, encrypted to the user's public key (if not already so), and stored in the user's database in an incoming message queue. The LEAP client then empties the incoming message queue, decrypting each message and saving it in the user's inbox, stored in local Soledad database. Since email is distributed to the client and stored via Soledad, all changes to the mailbox are synchronized to all devices.

For outgoing email, the LEAP client runs a thin SMTP proxy on the user's device, bound to *localhost*, and the mail user agent (MUA)[30] is configured to bind outgoing SMTP to *localhost*. When a SMTP proxy receives an email from the MUA, the SMTP proxy queries a local key manager (Nicknym agent) for the user's private key and public keys of all recipients. The message is then signed, and encrypted to each recipient. If a recipient's key is missing, email goes out in cleartext (unless user has configured the LEAP client to send only encrypted email). Finally, the message is relayed to provider's SMTP relay. The approach outlined here is similar to the approach taken by Garfinkel (2003) and Symantec,[31] although these systems do not include key discovery, key validation, encryption of incoming messages, secure storage, or synchronization of email among devices.

Future Research and Conclusion

The future work of LEAP has both a practical and research perspective. Once the system is launched, we expect feedback from users will be very instructive in determining what precise next steps the users should need. However, there is also a research agenda whose effects are vital to protecting the freedom of LEAP users, but whose ultimate goal is to remain invisible to these users: To tackle the problem of maintaining unmappability against the second threat model, a global passive adversary such as a well-funded national intelligence agency. In this threat model, the adversary is attempting to look at the timing and other characteristics of the encrypted messages in order to determine the social graph of the users.

(continued)

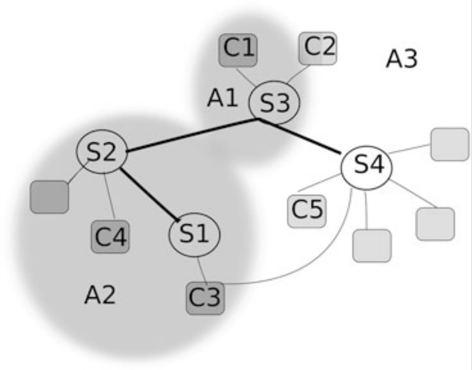
[30] Such as Thunderbird, Evolution, or Outlook.

[31] http://www.symantec.com/desktop-email-encryption

(continued)

Anonymity can be broken by virtue of statistical timing attacks where an adversary is observing traffic (Danezis and Serjantov 2004). For example, a scenario in which an attacker is observing traffic in a local jurisdiction between a client and a server (A_1), when an attacker is observing traffic, including server to server traffic (A_2), and when the attacker is a global passive adversary (A_3). Today users deploy very primitive techniques: Many users stay within trusted silos insofar as the email between different users on the same silo stays within the silo and so is not exposed to an adversary's traffic analysis powers. These three attacks are illustrated in Fig. 15.2, where servers are S and clients are C.

Fig. 15.2 Example of LEAP network



Luckily, email and even chat messaging have very much more relaxed latency constraints than the low latency and bursty traffic of web-browsing, and so a mix network could be used to provide anonymity (Dingledine and Syverson 2002). Given that the same LEAP software promotes interoperability between clients and servers as well as servers to servers, LEAP should at least be able to theoretically provide stronger anonymity by using cover traffic with proper padding and timing. As the traffic of LEAP has high latency and low volume traffic, we imagine we could use a version of the Drac adapted to a federated architecture (Danezis et al. 2010). While Drac has peer-to-peer architecture designed for a hostile network, a client-server approach assuming a network of trusted servers might be more realistic for deployment as it would not have the issues around NATs. Interestingly enough architecture that assumes a small group of trusted servers is structurally nearly equivalent to having supernodes in a peer-to-peer network, but with the added advantage that the traffic between servers will be 'thick,' i.e. frequent and of high-volume so that it will be easier to hide actual messages in constant-rate volume-based traffic. Unlike in Drac where the social graph of the user is revealed in

(continued)

(continued)

the first "friend-of-a-friend" routing needed to establish the circuit (Danezis et al. 2010) and avoid sybil attacks (Douceur 2002), in LEAP each client already has their first "friend" in the form of their trusted LEAP Platform. Far from being a merely administrative switch, a LEAP Platform has the added advantage of likely hosting a magnitude greater number of clients than any individual client will have in their social graph, but it is currently unknown whether a client-server version of Drac fares better or worse than a peer-to-peer version in terms of anonymity sets. Given the relatively small amount of servers likely participating in the LEAP network, it is unclear if a client-server version of Drac would require "epochs" for the circuit-building of onion-encrypted messages across the circuit (and so simply relying on Tor might be a good implementation choice) or if some variant of hop-by-hop encryption that takes advantage of the LEAP architecture should be used.

So far no mix networks have reached widespread deployment amongst users for their everyday usage. If LEAP is to make mix networking usable by the masses, it will have to carefully chose the parameters of volume-based constant-rate traffic. Ideally, the mix network would restrict communication to a background rate, but that background rate may differ between client-to-server and server-to-server hops. Also, the background rate may be constant timed but mix up two different constant rates, such as one constant rate that is low volume and relatively low latency (for mostly chat) with another constant rate for high volume and even higher latency traffic (mostly email), although all kinds of traffic (including key discovery and retrieval, perhaps as well as any other traffic through the EIP) should be mixed.

In the long-term, we would like encrypted messaging to be usable on the Web without installing client software such as the LEAP client. This will require the maturation of a secure (JavaScript) Web Cryptography API that can successfully prevent the private key material from being accessed by the server.[32] This allows encrypted messaging to be boot-strapped on top of existing Web clients rather than having to use native applications such as OpenVPN clients with a non-Web mail client (as in LEAP currently). Simply having the private keys of users on the server such as done by Lavabit is unacceptable as the keys can be rather easily compromised if the server itself is under compulsion or attacked.[33] Ultimately, anonymity loves company. For LEAP to be successful in fighting the surveillance by the powerful secret state, our technical solution must be majoritarian: Secure and anonymous messaging must serve the needs of all people, and be cheap and usable enough to become the default way of communicating on the Internet. First encrypted e-mail, then the world!

[32] http://www.w3.org/2012/webcrypto/

[33] http://www.thoughtcrime.org/blog/lavabit-critique/

References

Danezis, G., Diaz, C., Troncoso, C., Laurie, B.: Drac: An architecture for anonymous low-volume communications. In Atallah, M., Hopper, N., eds.: Privacy Enhancing Technologies. Volume 6205 of Lecture Notes in Computer Science. Springer Berlin / Heidelberg (2010) 202–219

Danezis, G., Serjantov, A.: Statistical disclosure or intersection attacks on anonymity systems. In: in Proceedings of 6th Information Hiding Workshop (IH 2004. (2004) 293–308

Dingledine, R., Syverson, P.F.: Reliable mix cascade networks through reputation. In Blaze, M., ed.: Financial Cryptography. Volume 2357 of Lecture Notes in Computer Science., Springer (2002) 253–268

Dingledine, R., Mathewson, N., Syverson, P.: Tor: The second-generation onion router. Proceedings of the 13th USENIX Security Symposium **2** (2004)

Douceur, J.R.: The sybil attack. In Druschel, P., Kaashoek, M.F., Rowstron, A.I.T., eds.: IPTPS. Volume 2429 of Lecture Notes in Computer Science., Springer (2002) 251–260

Greenwald, G.: No Place to Hide: Computer Hacking, Crashing, Pirating, and Phreaking. Metropolitan Books (2014)

Gaw, S., Felten, E.W., Fernandez-Kelly, P.: Secrecy, flagging, and paranoia: adoption criteria in encrypted email. In: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems. CHI '06, New York, NY, USA, ACM (2006) 591–600

Garfinkel, S.L.: Enabling email confidentiality through the use of opportunistic encryption. In: Proceedings of the 2003 annual national conference on Digital government research. dg.o '03, Digital Government Society of North America (2003) 1–4

Pouwelse, J.A., Garbacki, P., Wang, J., Bakker, A., Yang, J., Iosup, A., Epema, D.H.J., Reinders, M., van Steen, M.R., Sips, H.J.: Tribler: a social-based peer-to-peer system. Concurrency and Computation: Practice and Experience **20** (2008) 127–138

Whitten, A., Tygar, J.D.: Why johnny can't encrypt: a usability evaluation of pgp 5.0. In: Proceedings of the 8th conference on USENIX Security Symposium - Volume 8. SSYM'99, Berkeley, CA, USA, USENIX Association (1999) 14–14

Chapter 16
Enabling Privacy by Design in Medical Records Sharing

Jovan Stevovic, Eleonora Bassi, Alessio Giori, Fabio Casati, and Giampaolo Armellin

Abstract In healthcare a multiplicity of actors needs to access and share patients' data while being compliant with policies defined by data protection legislation. Building frameworks to enable stakeholders to design and develop data-sharing mechanisms in compliance with legislations is a challenging task.

In this work, we propose a methodology and a platform called CHINO, inspired by Privacy by Design principles, to guide the involved stakeholders during the definition of data-sharing processes by using visual representations such as Business Process Modelling (BPM). BPM enables the stakeholders to reason and share their understanding about privacy aspects from early analysis phases, while CHINO platform provides the execution framework for the defined BPM processes and privacy policies.

To prove the CHINO efficacy, we show how policies extracted from legislations can be modelled and executed and we report our studies with end-users with whom we validated the system usability. We analyse also CHINO from a legal point of view and its compliance with data protection legislations.

J. Stevovic (✉) • G. Armellin
Centro Ricerche GPI, Trento, Italy
e-mail: jovan.stevovic@cr-gpi.it; giampaolo.armellin@cr-gpi.it

E. Bassi
Department of Information Engineering and Computer Science, University of Trento, Trento, Italy

Nexa Center for Internet and Society, Polytechnic University of Torino, Trento, Italy
e-mail: bassi@disi.unitn.it

A. Giori
Fondazione Graphitech, Trento, Italy
e-mail: alessio.giori@graphitech.it

F. Casati
Department of Information Engineering and Computer Science, University of Trento, Trento, Italy
e-mail: casati@disi.unitn.it

S. Gutwirth et al. (eds.), *Reforming European Data Protection Law*,
Law, Governance and Technology Series 20, DOI 10.1007/978-94-017-9385-8_16

16.1 Introduction

Data sharing and interoperability among healthcare applications is fundamental to improve healthcare assistance.[1] Many projects such as the Italian Electronic Health Record (EHR) reference architecture,[2] UK NHS system, or the European epSOS project[3] have been proposed with the aim of interconnecting different applications. However, the development of such systems is challenging, and one reason is that they need to comply with strict privacy and compliance rules defined by Data Protection legislation.[4] While the projects mentioned above have considered the legislation during their development, to the best of our knowledge none of them have considered the privacy related aspects through all stages of project development as proposed by the Privacy by Design approach.[5] As a consequence, in some cases this led to critical privacy breaches[6] and limitations in their functionalities. For example, none of them gave to the data subjects (i.e. patients) the possibility to have full control over their data or transparency about data management aspects. Instead, considering privacy during the entire lifecycle of software development leads to multiple benefits such as providing more efficient security and privacy strategies, patient-centred privacy mechanisms and therefore improved customer satisfaction, trust, and more efficient operations.[7]

With the CHINO project we aim at creating a framework, inspired by Privacy by Design principles, to enable a multidisciplinary collaboration of various stakeholders involved in the design and development of data sharing mechanisms

[1] Richard Hillestad et al., "Can electronic medical record systems transform health care? Potential health benefits, savings, and costs," *Health Affairs* (2005): 24.

[2] Italian Data Protection Authority, *Guidelines on the Electronic Health Record. and the Health File*, [doc. Web 1634116] July 16, 2009, http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/export/1634116.

[3] epSOS European eHealth project, http://www.epsos.eu/; *Article 29 Data Protection Working Party, Working Document 01/2012 on epSOS*, Adopted on 25 January 2012, wp 189.

[4] *European Parliament and Council: Directive 95/46/EC: Directive on protection of individuals with regard to the processing of personal data and on the free movement of such data*; *Italian Data Protection Code: Legislative Decree No. 196/2003*. See also, *European Parliament and Council: Proposal for a regulation 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)*,2012; *European Parliament and Council: Directive 2011/24/EU: Directive on the application of patients' rights in cross-border healthcare*; See also Italian Ministry of Innovation and Technology, *InFSE: Technical Infrastructure for Electronical Health Record Systems, v1.2.*, 2012.

[5] Ann Cavoukian, "Privacy by Design," Information & Privacy Commissioner, Ontario, Canada. http://www.ipc.on.ca/images/Resources/privacybydesign.pdf. (2009).

[6] The Guardian, *NHS staff breach personal data 806 times in three years*, 2011. Available at: http://www.theguardian.com/healthcare-network/2011/oct/28/nhs-staff-breach-personal-data-806-times. Accessed on January 2014.

[7] Ann Cavoukian, "Privacy in the Clouds," *Identity in the Information Society* (2009): 1.

and to consider privacy, business and organisational requirements during all stages of software development; from analysis to deployment and execution. We aim at creating a data protection environment by moving privacy issues directly into the technology and the marketplace.[8] We envision that, by exploiting the advantages of visual representations such as Business Process Modelling (BPM) technology,[9] we can give to the stakeholders the necessary tools to reason and share their understanding about compliance aspects. Such representations should facilitate also the phases of project validations performed before going into production, and inspections by Compliance Officers at runtime.

In this direction, CHINO proposes a methodology that starts with the extraction of compliance requirements from legislations and with the gathering of business requirements from the involved stakeholders, and ends with the definition of executable processes that are able to enforce the collected requirements. At each step, the methodology guides the involved actors by giving them tools and guidelines on how to define processes and rules that are later executed into the CHINO execution environment.

The paper presents the CHINO methodology by considering a healthcare case study and privacy requirements extracted from Italian,[10] European[11] and HIPAA[12] legislations. We show examples of defined processes and report a user study with a group of developers that have tested the system usability by using notions from Human Computer Interaction discipline. We conclude by analysing the methodology with main focus on the steps in which compliance officers are involved in the definition of processes and validation of compliance against data protection laws.

The paper is organised as follows. Section 2 gives an overview of research effort in related areas. Section 3 presents the use case scenario and a first example set of extracted policies from legislations. The CHINO methodology, technology and its validation including the usability study are presented in Section 4. In section 5 we analyse CHINO from a legal point of view while in Section 6 we discuss the results and conclusions.

[8] Ann Cavoukian, "Personal Data Ecosystem (PDE) – A Privacy by Design Approach to an Individual's Pursuit of Radical Control," in *Digital Enlightenments Yearbook 2013. The Value of Personal Data*, ed. Mireille Hildebrandt et al. (IOS Press, 2013), 89–101.

[9] Activiti BPM Platform, Available at http://activiti.org/.; Richard Lenz and Manfred Reichert, "It support for healthcare processes premises, challenges, perspectives". *Data Knowledge Engineering* (2007): 61.

[10] *Legislative Decree No. 196/2003*.

[11] *Directive 95/46/EC*. See also, *European Parliament and Council: Proposal for a regulation 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)*.

[12] Office for Civil Rights. *HIPAA, medical privacy national standards to protect the privacy of personal health information*. 2000.

16.2 Related Work

Data sharing in healthcare is fundamental to improve the assistance services and many projects tried to address related challenges.[13] Commercial solutions such as PracticeFusion,[14] national projects such as the Italian EHR reference system,[15] the European project epSOS or the electronic social and health record developed for the Trentino region in Italy[16] are just some examples.

In such context process based technologies such as BPM have been demonstrated to be efficient in modelling and executing the assistance processes and activities that involve multiple users. The work by Richard Lenz and Manfred Reichert[17] analyses the impacts of process-based technologies on healthcare demonstrating their potential benefits on assistance services. The authors identify two kinds of processes: organisational processes and medical processes. In this work we analyse both types to define compliant data management processes to manage single medical records.

The work by Ottensooser et al.[18] shows that once defined and executed, BPM processes can also facilitate the verification activities by compliance officers. It analyses the understandability of a language for BPM called Business Process Model and Notation (BPMN), versus text notation for representing the design of information systems showing positive results. In another work by Recker and Dreiling[19] it is claimed that people, who know a business process notation, can switch to a new notation quite easily. We focus on enabling developers to create processes in an easy way and study their level of confidence following the methodologies and best practices in interaction design.[20]

[13] Richard Hillestad et al., “Can electronic medical record systems transform health care? Potential health benefits, savings, and costs,” *Health Affairs* (2005): 24.

[14] Practice Fusion, *Free Web-based Electronic Health Record*, www.practicefusion.com.

[15] Italian Ministry of Innovation and Technology, *InFSE: Technical Infrastructure for Electronical Health Record Systems, v1.2*. (2012).

[16] Giampaolo Armellin et al., “Privacy preserving event driven integration for interoperating social and health systems,” *Secure Data Management 7th VLDB workshop* (2010): 63–68.

[17] Richard Lenz and Manfred Reichert, “It support for healthcare processes premises, challenges, perspectives,” *Data Knowledge Engineering* (2007): 61.

[18] Avner Ottensooser et al., “Making sense of business process descriptions: An experimental comparison of graphical and textual notations,” *Journal of Systems and Software* (2012): 85.

[19] Jan C. Recker and Alexander Dreiling, “Does it matter which process modelling language we teach or use? An experimental study on understanding process modelling languages without formal education,” in *18th Australasian Conference on Information Systems* (University of Southern Queensland, 2007.

[20] See for instance Helen Sharp, “Interaction design,” (Wiley.com., 2003).

Some works uses BPM to tackle challenges related to privacy-aware data sharing.[21] The extracted and formally defined requirements and obligations from legislations can be synthesised as business processes[22] and work such as the one done by Bellamy et al.[23] demonstrates that with visual representations there could be benefits in understanding and improving them. The work by Lu et al.[24] shows an approach for compliance aware business process design while the work by Milosevic et al.[25] translates constrains and contracts into business processes. We chose to approach compliance related challenges proactively following the Privacy by Design[26] that has emerged as one of most promising approaches in tackling privacy related issues. Although it is only a set of high level principles and it has been criticised by some researchers due to its sometimes vague and high expectations,[27] it has been successfully applied in some projects and case studies.[28] Privacy by Design considers the privacy related aspects from early stages of systems design and has been introduced in the regulation framework by the Art. 29 Data Protection Working Party in the document *The Future of Privacy*[29] and in the *Proposal for the new European General Data Protection Regulation*. Therefore we aim at studying how the healthcare scenario proposed by the CHINO project can support and embed Privacy by Design principles, and if it can provide a reference implementation in this domain.

[21] Trevor Breaux et al., "Towards regulatory compliance: Extracting rights and obligations to align requirements with regulations," in *Requirements Engineering, 14th IEEE International Conference* (2006), 49–58.

[22] Ahmed Awad et al., "An iterative approach for business process template synthesis from compliance rules," *Advanced Information Systems Engineering* (2011): 6741.

[23] Rachel K. E. Bellamy et al., "Seeing is believing: designing visualizations for managing risk and compliance," *IBM System Journal* (2007): 46.

[24] Ruopeng Lu et al., "Compliance-aware business process design," *BPM Workshops* (2008): 4928.

[25] Zoran Milosevic et al., "Translating business contract into compliant business processes," in *EDOC'06* (IEEE Computer Society, 2006), 211–220.

[26] Ann Cavoukian, "Privacy by Design,", Information & Privacy Commissioner, Ontario, Canada. http://www.ipc.on.ca/images/Resources/privacybydesign.pdf. (2009); Ann Cavoukian, "Privacy in the Clouds," *Identity in the Information Society* (2009): 1; Peter Schaar "Privacy by Design," *Identity in the Information Society* (2010): 3.

[27] Bert-Jaap Koops and Ronald Leenes. "Privacy regulation cannot be hardcoded. A critical comment on the 'privacy by design' provision in data-protection law." International Review of Law, Computers & Technology ahead-of-print (2013): 1–13. See also, Ugo Pagallo. "On the Principle of Privacy by Design and its Limits: Technology, Ethics and the Rule of Law". European Data Protection 2012: 331–346.

[28] Paolo Balboni and Milda Macenaite, "Privacy by Design and anonymisation techniques in action: Case study of Ma3tch technology," *Computer Law and Security Review* (2013): 29; Antonio Kung et al., "Privacy-by-design in its applications," in *2nd Int. Workshop on Data Security and Privacy in Wireless Networks* (D-SPAN, 2011), 1–6.

[29] 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*, WP 168, (2009).

16.3 Use Case Scenario and Identified Policies

To test CHINO efficacy we started by analysing data-sharing scenarios and extracting privacy and compliance requirements from legislations. During the first CHINO testing,[30] sets of requirements were extracted from Italian and UK legislations and have been applied in a use case scenario called "doctor consultation". In this work, to further validate the framework, we consider European[31] and HIPAA legislations[32] and apply extracted requirements to a different use case called "immunisation scenario". The scenario involves different actors that need to share medical records about a patient:

> Mr Brown wants to spend his holidays in Mozambique and to be prepared for that environment, he asks to Dr Kelly, his family doctor, some advices. Dr Kelly alerts him that in Mozambique it is possible to get the typhus disease and she prescribes him a vaccine injection to administer before leaving. Dr Kelly creates an ePrescription using her medical record system, which uploads automatically the created record containing the ePrescription to CHINO. Then Mr Brown goes to the nearest hospital to get administered the vaccine. At the hospital, Dr Smith accesses Brown's medical data using his own medical record system that gets data from CHINO and administer the vaccine.

Next subsection describes privacy and compliance policies that have been extracted and that apply to this use case scenario.

16.3.1 Identified Policies

Extracting requirements and policies from legislations embeds some pitfalls starting from collecting the complete set of legislations and guidelines that are relevant to a considered project scenario. Moreover, these legal requirements and organizational policies should be compared and combined in order to identify their exact hierarchy and terms of applicability.[33] For example, the Italian context is characterized by many levels of authorities and rules which protect citizens privacy rights: starting from the EU level legislations[34] transposed in Italy with the Data Protection Code,[35] to the Guidelines and recommendations provided by the Italian Data Protection Authority in collaboration with the Ministry of Health on Electronic

[30] Jovan Stevovic et al., "Business process management enabled compliance-aware medical record sharing," *Int. J. Business Process Integration and Management* (2013):6.

[31] *Directive 95/46/EC.*

[32] Office for Civil Rights, *HIPAA, medical privacy national standards to protect the privacy of personal health information.*

[33] David G. Gordon, and Travis D. Breaux. "Reconciling multi-jurisdictional legal requirements: A case study in requirements water marking." *Requirements Engineering Conference*, IEEE, 2012.

[34] *Directive 95/46/EC.*

[35] *Legislative Decree No. 196/2003.*

Health Records.[36] Moreover each region has its own competences on applying healthcare legislation, which is done by many local healthcare providers called "ASL: Azienda Sanitaria Locale" that deliver assistance services to patients.[37] This context shows clearly that in Italy, like in other countries, there exist many bodies having different competences that define privacy legislations on different aspects.

Here we report a subset of privacy policies we extracted from legislation and that are relevant to the Immunisation scenario described before:

P1 a Data Controller (DC) must provide policies and procedures for the creation, maintenance, and revocation of access for both doctors and users.

P2 a DC must ensure that personal data may be processed only insofar as it is adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed.

P3 a DC must implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use PHI.

P4 a DC needs to ensure secure data management by implementing mechanisms for data encryption of Personal Health Information (PHI).

P5 a DC has the ability to disclose data for Research, Marketing, Fundraising only if appropriately de-identified by removing Personal Identifiable Information.

The identified requirements apply on the Immunisation scenario at different steps. During the doctors' access to patients' data, the P1, P2 and P3 policies need to be satisfied. The doctors need to have the required access rights (P1), access only to the information that is required to fulfil the tasks (P2) and their accesses need to be logged through audit mechanisms (P3). Patients' data need also to be kept secure on the systems used by the personal doctors, CHINO and the hospital systems (P4).

Next section describes the CHINO framework i.e., the methodology, the modelling framework and how BPM processes and rules are defined and executed based on the requirements and policies extracted insofar.

16.4 CHINO Framework

The main goal of CHINO is to provide a framework to involve different stakeholders (project managers, compliance and data protection officers, analysts and developers) through the lifecycle of development of compliant data sharing processes and

[36] Italian Data Protection Authority, *Guidelines on the Electronic Health Record*; Italian Ministry of Innovation and Technology, *InFSE: Technical Infrastructure for Electronical Health Record Systems, v1.2*. (2012).

[37] Giampaolo Armellin et al., "Privacy preserving event driven integration for interoperating social and health systems," *Secure Data Management 7th VLDB workshop* (2010): 6368; Municipality of Trento. *Regulations for the protection of personal data of the municipality of Trento*. http://www.comune.trento.it/, 2007; Municipality of Trento. *Operational guidelines to privacy*. http://www.comune.trento.it/, 2009.

privacy policies. The key idea sits in using BPM technology to define data management operations (e.g. storing, sharing) according to the data owners' requirements and policies extracted from laws and organizational rules. By doing so, CHINO executes the data owners' business processes and policies while replying to data requests and interacting with external applications and actors. In such way, CHINO enables a cross-organisation and even cross-border[38] compliance-aware medical record sharing since the processes and policies, for each of the participant organization, can be defined according to their own data protection legislation and set of requirements.

Next subsection shows how the CHINO methodology and how privacy law compliant data sharing can be achieved.

16.4.1 CHINO Methodology

To identify actors and a set of steps to define privacy law compliant processes and policies that are later executed into the CHINO platform, we propose the CHINO methodology (sketched in Fig. 16.1). It identifies main steps, the actors and artefacts that are produced and consumed at each step. It does not refer to any software development methodology (e.g. Waterfall, or Agile) since the steps could be also executed iteratively and it is not tied to any specific privacy law or legislation; therefore it should be applicable to any regulatory context.

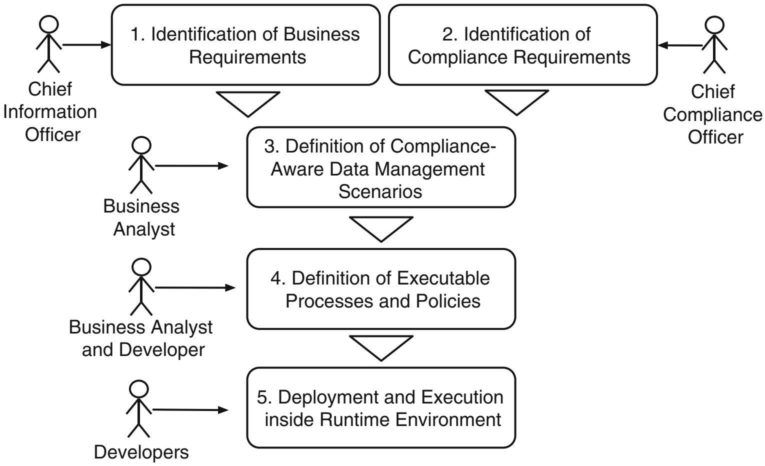

1. Identification of Business Requirements
2. Identification of Compliance Requirements
Chief Information Officer
Chief Compliance Officer
3. Definition of Compliance-Aware Data Management Scenarios
Business Analyst
4. Definition of Executable Processes and Policies
Business Analyst and Developer
5. Deployment and Execution inside Runtime Environment
Developers

Fig. 16.1 The CHINO methodology

[38] *Directive 95/46/EC* and in particular *Directive 2011/24/EU.*

The steps, as shown in Fig. 16.1 are:

1. Chief Information Officer identifies business requirements describing, for example, the flow of interactions, and tasks to be fulfilled by different actors or organisations. Such requirements, like in the Immunisation scenario, are often described in natural language with operational models describing how actors interact among them and with the medical record systems. At this step also domain experts such as doctors and nurses could be involved in defining the assistance processes and the data that need to be managed and shared.[39]
2. Chief Compliance Officer of the organisation identifies the legislation and extracts the compliance requirements including the security and privacy policies that need to be satisfied. For example, as shown by the use case, it could define at each step which security and privacy policies need to be applied, according to the applicable law (national, European, and international), and identifies exceptional cases in which data can be disclosed without patients' authorisations (policy P5 in Section 3.1). Due to legislation intrinsic complexity, the Compliance Officer could rely on collaborations and consultations with actors having a legal background to extract all requirements. This step could consist of various interactions also among compliance and information officers to devise the set of information that will be managed, the operations and the set of norms that will apply to such operations.
3. Business Analyst combines business requirements and compliance requirements to devise a high-level representation that describes the steps the involved parties should follow.[40] The business analyst can also annotate such representations with the corresponding security and privacy policies identified at Step 2.[41] If necessary, the step 2 and 3 can be performed more times iteratively to refine the policies to be enforced.[42]
4. Business Analyst and System Developer translate high-level representations into executable business processes and rules. Business processes implement the business logic of data management operations such as *Push Record* and *Get*

[39] Giampaolo Armellin et al., "Privacy preserving event driven integration for interoperating social and health systems," *Secure Data Management 7th VLDB Workshop* (2010): 6368.

[40] Alberto Siena et al., "Establishing regulatory compliance for IS requirements: an experience report from the health care domain," *29th Int. Conf. on Conceptual Modelling* (2010): 6412.

[41] Richard Lenz and Manfred Reichert, "It support for healthcare processes premises, challenges, perspectives," *Data Knowledge Engineering* (2007): 61.

[42] We give examples of such representations in Jovan Stevovic et al., "Business process management enabled compliance-aware medical record sharing," *Int. J. Business Process Integration and Management* (2013):6; but also leave to the users the freedom to choose the most appropriate representation according to the recommendations by Article 29 Data Protection Working Party, *Working Document on the processing of personal data relating to health in Electronic Health Records (EHR)*, Adopted on 15/02/2007, wp 131.; Ruopeng Lu et al., "Compliance-aware business process design" *BPM Workshops* (2008): 4928; Alberto Siena et al., "Establishing regulatory compliance for IS requirements: an experience report from the health care domain," *29th Int. Conf. on Conceptual Modelling* (2010): 6412.

Record. The defined security and privacy rules that are incorporated into business process steps are executed through operations on internal CHINO components.

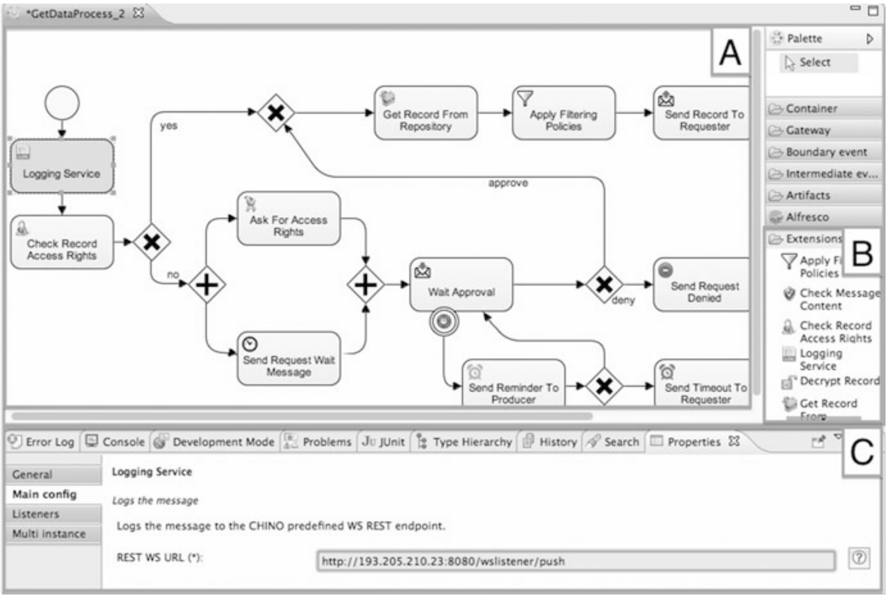
5. Finally, the resulting executable business processes and rules are deployed and executed into the shared execution environment.

In summary, the CHINO methodology identifies the sequence of steps carried out by multiple stakeholders, from high-level business requirement collection to the low-level process execution and policy enforcement. Next subsection shows the technology to support the process modelling.

16.4.2 CHINO Modelling Framework

The process and policy Modelling Framework, as described by the methodology, involves the collaboration of Business Analysts and Developers. Figure 16.2 shows the framework at work.

Developers can model processes in Section A by using a set of Business Process Model and Notation (BPMN)[43] modelling elements that can be dragged and



Logging Service

Logs the message

Logs the message to the CHINO predefined WS REST endpoint.

REST WS URL (*): http://193.205.210.23:8080/wslistener/push

Fig. 16.2 A screenshot of the CHINO Modelling Framework based on the (Activiti Designer Activiti BPM Platform, Available at http://activiti.org/)

[43] OMG, *BPMN–Business Process Model and Notation v2.0 Specification*, 2011, Available at http://www.omg.org/spec/BPMN/2.0/.

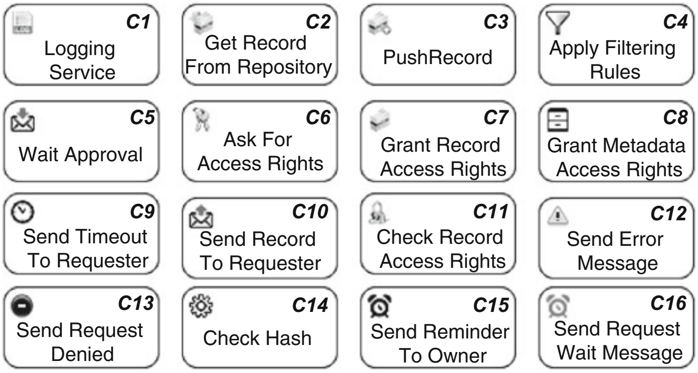


Fig. 16.3 A subset of the CHINO Custom Tasks

dropped from Section B. They will need to input some configuration parameters in the *Properties* tab shown in Section C to make it executable. Once deployed, the processes become automatically executable to manage organisations' data. The Modelling Framework is implemented by extending the Activiti Designer[44] with a set of new constructs called *Custom Tasks* to provide a comprehensive set of elements and to facilitate process modelling. Custom tasks are extensions to the standard BPMN 2.0 elements and a subset of them is shown in Fig. 16.3.

Each of the introduced custom tasks has a specific name, icon and behaviour. The set of custom modelling elements has been introduced to simplify the development of specific CHINO processes that implement data management operations. Namely, each of the custom tasks can be used either to reply to the requester with a specific and predefined message or to interact with the platform internal components.[45] They are used to define how patients' personal information is disclosed to, and managed by CHINO and how it is disclosed to other institutions and users. A subset of custom elements is described below:

- C1 – *Logging Service* is a customisable logging task that logs process status on internal Logging component or an external auditing system. It takes in input a customizable set of information that can be specified by the developers.
- C2 – *Get Record From Repository* restores the requested record from record store. The record store can be also external.[46]
- C3 – *Push Record* saves a record on the internal record store component.

[44] Activiti BPM Platform, Available at http://activiti.org/.

[45] For a more exhaustive technical description see Jovan Stevovic et al., "Business process management enabled compliance-aware medical record sharing," *Int. J. Business Process Integration and Management* (2013):6.

[46] According to new rules proposed by *European Parliament and Council: Proposal for a regulation 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).*

- C4 – *Apply Filtering Rules* applies purpose-based filtering rules to records to eliminate the unnecessary data based on the specified purpose of use.[47] This is fundamental to achieve the proportionality principle and satisfy the policy P2.

The following subsection shows how these elements were used within a process example to implement an operation according to identified requirements.

16.4.3 A Process Example

Here we show an example of a process that is executed inside the CHINO platform to implement an operation over data. We analyse in particular the *Get Record* operation that is invoked when a medical record is requested by an organisation. The process model in Fig. 16.4 (simplified for readability reason) has been implemented according to policies extracted from HIPAA legislation and listed in section 3.1.

It starts by checking the request message content to ensure that the request contains all the mandatory data. According to policies P1, P2 and P3 from Section 3.1, the request needs to be authorised, it needs to access only to the data the requester is entitled to access for that specific task and, all actions need to be logged. If the requester does not have the required access rights, the process will ask for approval to the record owner. Under HIPAA, usually personal doctors approve requests to data on behalf of the patients. Therefore, the process will wait for approval soliciting the doctor periodically. In case of approved request, the process retrieves the requested record from a local record store. The record store could be also remote in case this is mandated by guidelines for EHR creation or laws.[48] Once retrieved the record, the process needs to satisfy the proportionality principle

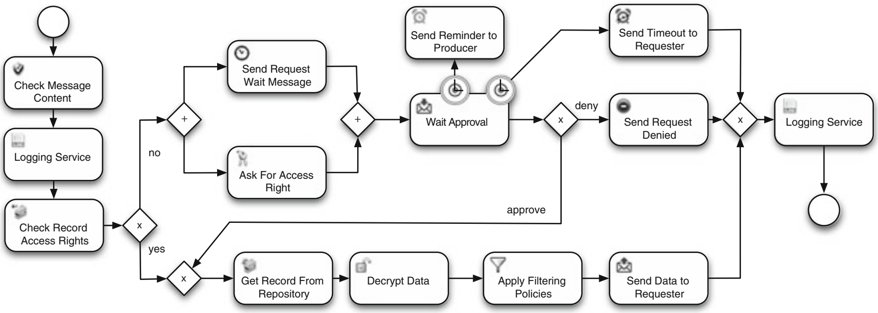


Fig. 16.4 The CHINO "*Get Record*" Process

[47] Giampaolo Armellin et al., "Privacy preserving event driven integration for interoperating social and health systems," *Secure Data Management 7th VLDB Workshop* (2010): 6368.

[48] This is the case of Italian law: Italian Ministry of Innovation and Technology, *InFSE: Technical Infrastructure for Electronical Health Record Systems, v1.2*. (2012).

that is one of the most important principles identified by Data Protection legislations and that needs to be tackled in combination with the principles of necessity and purpose limitation.[49] To satisfy those requirements, the process invokes the *Apply Filtering Policies* element that filters the data that is not necessary for that requestor for that specific purpose of access. The filtering policies are defined by record owners or entities responsible for record management (e.g. Data Controllers).[50] The record is then returned to the requestor replying to *Get Record* request. In case of request denied, a negative response is returned to the requester, while in case of timeout (neither positive nor negative response) a timeout message is returned. Finally in case something went wrong, an error message is returned.

The proposed process based approach is able also to manage easily the exceptional cases in which data subjects are under a certain age threshold or the records are about mental problems and should not be disclosed to the subjects. The defined processes are then deployed and executed in the CHINO Platform.

16.4.4 CHINO Platform

Following the CHINO methodology, once processes are defined (Step 4), they are deployed and executed inside the shared execution environment (Step 5). CHINO platform provides the execution environment and a set of internal components to manage data and rules. The platform is also responsible for technical aspects such as reliability, scalability, and secure communication with external systems.[51]

The platform prototype has been developed and tested by integrating it with a popular medical record system called OpenMRS (www.openmrs.org) and by developing the doctor consultation use case according to Italian and UK legislations. We defined data sharing processes in compliance to Italian and UK legislations and executed them inside CHINO to demonstrate that with CHINO, organisations are able to share medical records while being compliant with privacy legislations and while satisfying their internal business requirements.[52] This scenario demonstrated also how CHINO can enable cross-border and cross-legislation medical data sharing, according to Directive 2011/24/UE.

Next subsection shows how we analysed legislations in this work and how we tested process modelling with developers.

[49] Office for Civil Rights. *HIPAA, medical privacy national standards to protect the privacy of personal health information*.

[50] Giampaolo Armellin et al., "Privacy preserving event driven integration for interoperating social and health systems," *Secure Data Management 7th VLDB Workshop* (2010): 6368.

[51] Jovan Stevovic et al., "Business process management enabled compliance-aware medical record sharing," *Int. J. Business Process Integration and Management* (2013):6.

[52] Jovan Stevovic et al. "Business process management enabled compliance-aware medical record sharing," *Int. J. Business Process Integration and Management* (2013):6.

16.4.5 The Usability Validation

According to the CHINO methodology, Business Analysts and Developers should be able to define the processes in compliance to the identified requirements by using the Modelling Framework. To test these assumptions and the Modelling Framework usability, we performed a user study with a group of nine developers that had preliminary knowledge about process modelling with the standard BPMN Activiti Designer.[53] With the user study we tried to understand if the requirements identified at Steps 1, 2 and 3 can be mapped into business processes at Step 4. The users where chosen among master students and employees of the University of Trento. The analysis was based on notions from the Interaction Design (ID) studied in Human Computer Interaction (HCI) discipline and applying the usability testing methodology called Think Aloud.[54] According to it, the standard usability test is performed recording users' performance on an assigned task. In our test we showed to users a document explaining the CHINO framework, the Immunisation scenario and a list of identified requirements. We monitored and stimulated them to speak while performing the assigned tasks to analyse their behaviour.

At the end of the test we asked them to fill a questionnaire about overall satisfaction about the assigned tasks which had two types of responses. The first one in a scale from 1 to 7 points where 1 correspond to negative opinion such as *Strongly Disagree* and 7 to a positive judgement such as *Strongly Agree*. The second type was in form of open questions. All the numeric questions were mandatory while the open ones were optional. We report some questions while the complete questionnaire including a detailed analysis of results can be found here[55]:

Q1 "Overall, I am satisfied with the ease of completing the exercise in this scenario."
Q10 "I was able to complete the exercise quickly using this system."
Q21 "This system has all the functions and capabilities I needed."
Q23 "It was easy to understand the concepts introduced by this framework."
Q25 "How do you rate the overall experience with the CHINO Modelling?"

16.4.5.1 Study Results

To evaluate the responses for each question we calculated the mean (μ_n) and variance ($\sigma_n{}^2$) where the first coefficient expresses the positive or negative opinion of the users, while the second represent the level of disagreement among users.

[53] Activiti BPM Platform, Available at http://activiti.org/.

[54] Helen Sharp, "Interaction design," (Wiley.com., 2003).

[55] Alessio Giori, "Design, development and validation of a methodology and platform for compliance-aware medical record management", Master's degree thesis at University of Trento, 2013.

Test showed a positive impression about the Modeller usage after a few times it has been used. However, when users used it for the first time some differences among opinions emerged. Only two users expressed an overall negative feedback about their performance, however, since they were able to perform their tasks, this does not represent an important limitation, although it suggests us to take into consideration developing a strategy to train new users.

An example of a positive feedback within open questions is:

> I am comfortable with the diagrams because it really represents the information which is held on hospitals.

And also some negative ones:

> The framework as I said is easy to use but anyway I had some problems of stability during the usage, so for this reason, relatively to the question if I would recommend this tool to others the real answer is yes, but . . .

The stability issues are related to the Activiti Designer and not to our specific extension and it is just a matter of software maturity since Activiti project is being frequently updated with newer versions.

Overall, the study gave us important feedback about custom task usability and suggested some improvements especially regarding the explanation of their usage. Other suggestions include also the need for better explanation of usage of combinations of different tasks to achieve a specific goal. In conclusion, tests showed a satisfactory usability level of the Modelling Framework and demonstrated that users were able to transpose requirements into processes while underlining the need for smaller improvements of the CHINO platform.

Tests validated the technical usability and feasibility of the CHINO approach, while the next section analyses how CHINO achieves privacy law compliance.

16.5 Privacy Law Compliance with CHINO

Here we analyse CHINO from the legal point of view and reason about its ability to preserve privacy and data protection rights and to support compliant process definition. We show how CHINO can help in achieving the identified goals by answering in particular to the following two macro-questions:

1. If CHINO provides technological elements (modeller, modelling elements, internal components) to support the development of privacy law compliant healthcare data management processes and policies.
2. If CHINO process based approach could facilitate the tasks (emphasised in Fig. 16.5) of process and policy approvals or verifications. These activities are typically done before going into production phase or in case of legally motivated inspections by Compliance Officers at runtime.

In order to answer to the first question we summarize here how CHINO technology and, more in general, the process based approach it proposes, can satisfy

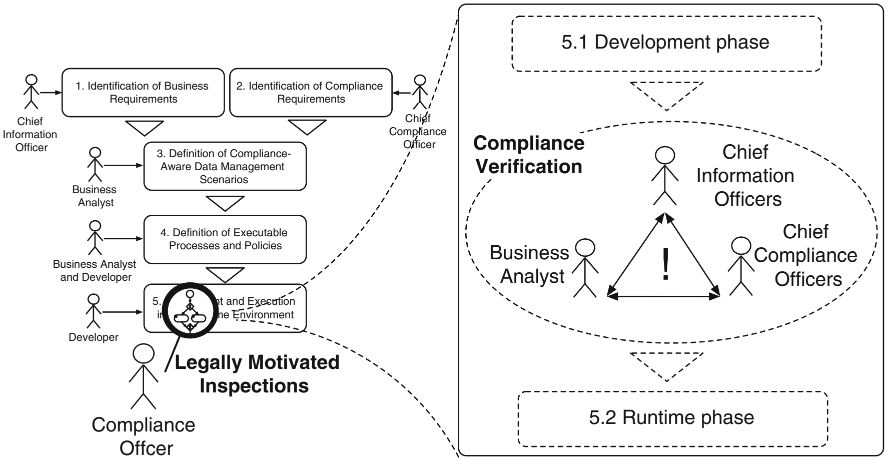

1. Identification of Business Requirements
2. Identification of Compliance Requirements
Chief Information Officer
Chief Compliance Officer
3. Definition of Compliance-Aware Data Management Scenarios
Business Analyst
4. Definition of Executable Processes and Policies
Business Analyst and Developer
5. ...t and Execution in ...he Environment
Developer
Legally Motivated Inspections
Compliance Offcer
5.1 Development phase
Compliance Verification
Chief Information Officers
Business Analyst
Chief Compliance Officers
!
5.2 Runtime phase

Fig. 16.5 CHINO Methodology with the focus on compliance inspections and verifications

the set of requirements extracted from the Italian legislation, directives and set of guidelines for the creation of Electronic Health Record (EHR) systems. We start by analysing the set of recommendations of the Art. 29 Data Protection Working Party in *Working Document 01/2012 on epSOS,*[56] and in *Working Document on the processing of personal data relating to health in Electronic Health Records (EHR).*[57] Art. 29 Working Party provides recommendations on several topics emphasising the need for special safeguards in order to guarantee the data protection rights of patients and individuals. Some recommendations include the respect for data subjects' self-determination and authorisation procedures, security measures, transparency, liability issues and finally, the availability of mechanisms to control the data processing.

As described in the paper, CHINO aims at providing a framework to support the privacy by design approach while providing tools and mechanisms to define data management processes and policies. In such way, CHINO proposes a proactive approach in accordance to the privacy by design principles by providing effective technical and organisational tools for healthcare institutions to consider privacy related aspects during the whole project lifecycle.[58]

[56] Article 29 Data Protection Working Party, *Working Document 01/2012 on epSOS*, Adapted on 25 January 2012, wp 189.

[57] Article 29 Data Protection Working Party, *Working Document on the processing of personal data relating to health in Electronic Health Records (EHR),* Adopted on 15 February 2007, wp 131.

[58] Ann Cavoukian, "Personal Data Ecosystem (PDE) – A Privacy by Design Approach to an Individual's Pursuit of Radical Control," In *Digital Enlightenments Yearbook 2013. The Value of Personal Data*, ed. Mireille Hildebrandt et al. (IOS Press, 2013), 89–101.

Analysing more deeply CHINO with the focus on data protection requirements, it appears to be an appropriate platform for sharing personal and healthcare data also among organizations that belong to different regulatory contexts.[59] The flexibility provided by business process technology enables users to customize data management processes and data protection strategy according to their requirements.

From the data security point of view, CHINO technology provides the necessary mechanisms to satisfy the security requirements related to healthcare data management in the Italian scenario. In particular, the architectural features and capabilities have been built following the national level guidelines for EHR creation[60] and international standards such as IHE.[61] Therefore CHINO satisfies the requirements according to Articles 31 and 33ff of the Italian Data Protection Code,[62] and the release of a Privacy Impact Assessment.[63] It implements technical and organisational features to avoid loss or unauthorised alteration, processing and access to data. Furthermore it respects data protection general principles from the Directive 95/46/EC, and in particular the principles of purpose limitation, proportionality, data quality, necessity and the data subject's rights.

CHINO is able to enforce the *explicit consent* policy that is defined as the data subjects' explicit consent on the processing of their data and it is an exemption to the general prohibition to personal data processing, according to European legislation (Art. 8, Directive 95/46/EC).[64] CHINO access right policies and the assurance mechanism enable data subjects to freely express explicit, specific and informed consent about data sharing. According to the legislation, in special cases data can be processed without consent (e.g. compliance with legal obligations, protect vital interest of data subject, public interests). This is possible in CHINO by defining special conditions on the *Check Access Right* modelling element. Processes can be also defined to delegate the disclosure of data to data subjects' personal doctors. Data subjects could also delete and block data sharing (as required for instance by Art. 7, Italian Data Protection Code). Moreover the involved actors are able to receive notifications about the process status, including the requests of access. The updates of wrong data to assure data quality policy according to Italian, European and HIPAA legislations, are done through the *Push Record* task.

[59] *Directive 2011/24/EU.*

[60] Italian Ministry of Innovation and Technology, *InFSE: Technical Infrastructure for Electronical Health Record Systems, v1.2*. (2012).

[61] Integrating the Healthcare Enterprise (IHE), "IHE IT infrastructure (ITI) technical framework", Integration Profiles, v. 8, (2011).

[62] *Legislative Decree No. 196/2003.*

[63] *European Parliament and Council: Proposal for a regulation 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).* (2012).

[64] Article 29 Data Protection Working Party, *Opinion 15/2011 on the definition of consent*, Adopted on 13 July 2011, wp 187.

According to European legislation (Art. 6 of Directive 95/46/EC) and to the Italian Data Protection Code (Art. 11), personal data can only be processed for specified explicit and legitimate purposes and may not be processed further in a way incompatible with those purposes. CHINO provides technical tools for enabling data controllers to check step-by-step the lawfulness of the personal data process following the purpose principle[65]; the legitimate purposes of the process are recorded and all the access requests are filtered according to them. CHINO provides mechanisms to release data only according to the specified, explicit and legitimate purposes through the definition of filtering policies. Namely, the CHINO filtering task provides anonymisation mechanisms to remove sensible information on a purpose-based approach. For example in case the data need to be used for statistical purposes, a filtering policy that eliminate personal identifiable information can be defined.[66] These purpose-based policies can be defined quite easily in healthcare domain given the availability of the taxonomy of possible purposes for which healthcare data can be requested and used.[67]

By analysing more deeply the data security features, CHINO guarantees confidentiality and integrity of information against unauthorised access, disclosure or alterations. Moreover, it improves personal data traceability, so that each communication and each data transaction can be tracked back to a certain entity that can be easily audited. In order to assure data traceability, CHINO provides features to clearly identify all the actors and entities involved in the process execution. This allows identifying data controllers and data processors (and other involved entities) when executing operations over data and addressing specific and defined liabilities to data controllers and processors at any step of the processing. Logging ensures accountability on operations over data in compliance with the Italian Data Protection Code (Articles 28ff) and with the Guidelines on the EHR development.[68]

CHINO allows data controllers to keep privacy-sensitive data on their own servers if they have restrictions about data storage administrative locations, as it is the case in Italy.[69] Regarding the data stored inside CHINO, it is encrypted with standards algorithms (e.g. AES-128 and SHA-258 for hashing). The deployment of CHINO could be done also in Cloud-based environments. Although this aspect

[65] Article 29 Data Protection Working Party, *Opinion 3/2013 on purpose limitation*, Adopted on 2 April 2013, wp 203.

[66] Giampaolo Armellin et al., “Privacy preserving event driven integration for interoperating social and health systems,” *Secure Data Management 7th VLDB Workshop* (2010): 6368; Jovan Stevovic et al., “Business process management enabled compliance-aware medical record sharing,” *Int. J. Business Process Integration and Management* (2013):6.

[67] Italian Ministry of Innovation and Technology, *InFSE: Technical Infrastructure for Electronical Health Record Systems, v1.2*. (2012).

[68] Italian Data Protection Authority, *Guidelines on the Electronic Health Record.*

[69] Italian Data Protection Authority, *Guidelines on the Electronic Health Record.*

needs a deeper analysis, the combination of the possibility to decentralise record storage and encryption techniques satisfy the requirements recommended by Art. 29 Working Party in 2007.[70]

Relatively to the second question, we tried to analyse the healthcare software lifecycle that is depicted in Fig. 16.5 with particular focus on the compliance aspects that have been underlined in two specific phases. Namely, Fig. 16.5 shows the situations where the "Chief Compliance Officer", that is usually a privacy expert or a Data Protection Officer, is involved in the verification of the business processes developed at Step 5 and has the responsibility to approve or reject them. The other situation is related to recent Inspection Plan undertaken by the Italian Data Protection Authority in which medical record systems has been included as one of the potentially analysed systems.[71] This means that the Data Protection Authority will seek for documentation to check if the data lifecycle and data management procedures are compliant with legislation in order to assure protection to data subjects' rights.

Both situations shown in Fig. 16.5, describe tasks that could have significant impact on projects developed without considering exhaustively privacy related aspects (i.e. fines to responsible organizations or, in extreme cases, systems suspension or disposal).

To answer to this question we focus on the analysis of the CHINO technology and understanding if it could provide more transparency, documentation and details about the data management lifecycle in case of verifications and inspections. We focus mainly on the analysis of the BPM technology, as the core innovative technology, that can facilitate inspection procedures. Due to its visual representations, CHINO data management operations can be easily verified even by people with non-technical background such as Compliance Officers. Similarly to other scenarios and context,[72] visual representations can simplify the process of revision by lawyer and privacy experts due to its simplification of understanding for people with non IT background. CHINO expresses in a more clear way which privacy requirements are satisfied when compared to standard textual documentation making easier to identify different steps and related rights, duties and liabilities.

[70] Article 29 Data Protection Working Party, *Working Document on the processing of personal data relating to health in Electronic Health Records (EHR),* Adopted on 15 February 2007, wp 131.

[71] Italian Data Protection Authority, *Newsletter about the Inspection Plan. February 14 2013*, Available at http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/2256479.

[72] Rachel K. E. Bellamy et al., "Seeing is believing: designing visualizations for managing risk and compliance," *IBM System Journal* (2007): 46; Avner Ottensooser et al., "Making sense of business process descriptions: An experimental comparison of graphical and textual notations," *Journal of Systems and Software* (2012): 85; Jan C. Recker and Alexander Dreiling, "Does it matter which process modelling language we teach or use? An experimental study on understanding process modelling languages without formal education," in *18th Australasian Conference on Information Systems* (University of Southern Queensland, 2007).

16.6 Conclusions

Privacy law compliance is a challenging and complex goal to achieve while developing IT solutions that manage and share sensitive data. This paper shows how CHINO framework is able to tackle compliance issues in medical data sharing by exploiting the advantages of visual representations such as BPM technologies.

By performing different tests; starting with extracting policies from Italian, European and HIPAA legislations, modelling and executing corresponding processes and policies and with user studies, we have proved the overall CHINO methodology and technology applicability and its soundness relatively to Privacy by Design principles. From the privacy legislation analysis has emerged that CHINO provides all the necessary features to develop data management processes that are compliant with examined legislations. In addition, the BPM technology simplifies the process development and revision tasks that are done by Compliance Officers. The adoption of the same visual representations from the first stages of analysis up to the execution, simplifies the collaboration and sharing of knowledge among stakeholders with different backgrounds.

A potential evolution of the CHINO platform is the deployment on Cloud-based infrastructures to give to users the possibility to define their own data management strategies for their personal data. It could also enable users and organisations to share processes among them and collaboratively improve them.

Furthermore, the proposed solution, and in particular the positive validation with privacy experts, enabled us to apply the CHINO methodology (and potentially also the technology) into industrial projects. Namely, we are currently adopting the CHINO methodology and BPMN diagrams as the documentation technology to interact with stakeholders (i.e., analysts, assistance providers, governance and compliance experts from a legal consulting firm). The initial feedback about the proposed approach suitability is extremely positive and the reporting of these experiences will be part of the future work on this project.

References

Activiti BPM Platform, Available at http://activiti.org/.

Armellin, Giampaolo, Dario Betti, Fabio Casati, Annamaria Chiasera, Gloria Martìnez, and Jovan Stevovic. “Privacy preserving event-driven integration for interoperating social and health systems.” In *Proceedings of the 7th VLDB Conference on Secure Data Management, SDM’10,* 6368 (2010): 54–69.

Article 29 Data Protection Working Party, *Working Document 01/2012 on epSOS*, Adopted on 25 January 2012, wp 189. (2012)

Article 29 Data Protection Working Party, *Working Document on the processing of personal data relating to health in Electronic Health Records (EHR)*, Adopted on 15 February 2007, wp 131. (2007)

Article 29 Data Protection Working Party, *Opinion 15/2011 on the definition of consent*, Adopted on 13 July 2011, wp 187. (2011)

Article 29 Data Protection Working Party, *Opinion 3/2013 on purpose limitation*, Adopted on 2 April 2013, wp 203. (2013)

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*, wp 168. (2009)

Awad, Ahmed, Rajeev Goré, James Thomson, and Matthias Weidlich., "An iterative approach for business process template synthesis from compliance rules." In *Advanced Information Systems Engineering, LNCS* 6741 (2011): 406–421

Balboni, Paolo, and Milda Macenaite. "Privacy by Design and anonymisation techniques in action: Case study of Ma^{3}tch technology." *Computer Law and Security Review* 29, (4) (2013): 330–340

Bellamy, Rachel K. E., Thomas Erickson, Brian Fuller, Wendy A. Kellogg, Rhonda Rosenbaum, John C. Thomas, and Tracee Vetting Wolf. "Seeing is believing: designing visualizations for managing risk and compliance." *IBM System J.* 46(2) (2007): 205–218

Breaux, Travis D, Matthew W. Vail, Annie I. Anton. "Towards regulatory compliance: Extracting rights and obligations to align requirements with regulations." In *Requirements Engineering, 14th IEEE International Conference* (2006): 49–58

Cavoukian, Ann, "Privacy by Design." Information & Privacy Commissioner, Ontario, Canada http://www.ipc.on.ca/images/Resources/privacybydesign.pdf. (2009)

Cavoukian, Ann, "Privacy in the Clouds." *Identity in the Information Society* 1(1) (2009): 89–108

Cavoukian, Ann "Personal data Ecosystem (PDE) – A Privacy by Design Approach to an Individual's Pursuit of Radical Control." In *Digital Enlightenment Yearbook 2013: The Value of Personal Data*, edited by Mireille Hildebrandt et al., 89–101. IOS Press: 2013

European Parliament and Council: Directive 95/46/EC: Directive on protection of individuals with regard to the processing of personal data and on the free movement of such data

European Parliament and Council: Directive 2011/24/EU: Directive on the application of patients' rights in cross-border healthcare

European Parliament and Council: Proposal for a regulation 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)

epSOS European eHealth project, http://www.epsos.eu/

Gordon, David G., and Travis D. Breaux. "Reconciling multi-jurisdictional legal requirements: A case study in requirements water marking." *Requirements Engineering Conference*, IEEE, 2012.

Hillestad, Richard, James Bigelow, Anthony Bower, Federico Girosi, Robin Meili, Richard Scoville, and Roger Taylor. "Can electronic medical record systems transform health care? Potential health benefits, savings, and costs." *Health Affairs* 24(5) (2005) 1103–1117

Integrating the Healthcare Enterprise (IHE), "IHE IT infrastructure (ITI) technical framework", Integration Profiles, v. 8, (2011)

Italian Data Protection Authority. *Guidelines on the Electronic Health Record and the Health File*, [doc. Web 1634116] July 16, 2009, http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/export/1634116

Italian Data Protection Authority. *Newsletter about the Inspection Plan. February 14 2013*, Available at http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/2256479

Italian Ministry of Innovation and Technology. *InFSE: Technical Infrastructure for Electronical Health Record Systems, v1.2.* (2012)

Legislative Decree No. 196/2003

Koops, Bert-Jaap, and Leenes, Ronald. "Privacy regulation cannot be hardcoded. A critical comment on the 'privacy by design' provision in data-protection law." *International Review of Law, Computers & Technology* (2013): 1–13.

Kung, Anthony, Johann C. Freytag, and Frank Kargl. "Privacy-by-design in its applications." In *IEEE International Symposium on World of Wireless, Mobile and Multimedia Networks (WoWMoM),* IEEE. 1–6.

Lenz, Richard, and Manfred Reichert. “It support for healthcare processes premises, challenges, perspectives.” *Data Knowledge Engineering* 61(1) (2007): 39–58

Lu, Ruopeng, Shazia Sadiq, and Guido Governatori. “Compliance-aware business process design.” *BPM Workshops* 4928 (2008): 120–131

Milosevic, Zoran, Shazia Sadiq, and Maria E. Orlowska. “Translating business contract into compliant business processes.” In *EDOC’06*, 211–220, IEEE Computer Society, 2006

Municipality of Trento. *Regulations for the protection of personal data of the municipality of Trento*. http://www.comune.trento.it/, 2007. Accessed: 2013-12-20.

Municipality of Trento. *Operational guidelines to privacy*. http://www.comune.trento.it/, 2009. Accessed: 2013-12-20.

Office for Civil Rights. *HIPAA, medical privacy national standards to protect the privacy of personal health information*, 2000

OMG. *BPMN - Business Process Model and Notation v2.0 Specification* (2011), Available at http://www.omg.org/spec/BPMN/2.0/.

Ottensooser, Avner, Alan Fekete, Hajo A. Reijers, Jan Mendling, and Con. Menictas. “Making sense of business process descriptions: An experimental comparison of graphical and textual notations.” *Journal of Systems and Software* 85(3) (2012): 596–606

Pagallo, Ugo. “On the Principle of Privacy by Design and its Limits: Technology, Ethics and the Rule of Law”. *European Data Protection* 2012: 331–346

Practice Fusion, *Free Web-based Electronic Health Record*, www.practicefusion.com.

Recker, Jan C., and Alexander Dreiling. “Does it matter which process modelling language we teach or use? An experimental study on understanding process modelling languages without formal education.” In *18th Australasian Conference on Information Systems*, University of Southern Queensland, (2007).

Schaar, Peter.“Privacy by Design.” *Identity in the Information Society* 3(2) (2010): 267–274

Siena, Alberto, Giampaolo Armellin, Gianluca Mameli, John Mylopoulos, Anna Perini, and Angelo Susi. “Establishing regulatory compliance for IS requirements: an experience report from the health care domain.” *29th Int. Conf. on Conceptual Modelling*, 6412 (2010): 90–103

Sharp, Helen. “Interaction design.” Wiley.com. (2003)

Stevovic, Jovan, Jun Li, Hamid Motahari-Nezhad, Fabio Casati, Giampaolo Armellin. “Business process management enabled compliance-aware medical record sharing.” *Int. J. Business Process Integration and Management* 6(3) (2013): 201–223

The Guardian, *NHS staff breach personal data 806 times in three years*, 2011, Available at: http://www.theguardian.com/healthcare-network/2011/oct/28/nhs-staff-breach-personal-data-806-times. Accessed on January 2014.