> Internet Privacy

Options for adequate realisation

Johannes Buchmann (Ed.)

acatech STUDY

Springer Vieweg

acatech
NATIONAL ACADEMY OF
SCIENCE AND ENGINEERING

> Internet Privacy

Options for adequate realisation

Johannes Buchmann (Ed.)

acatech STUDY
May 2013

acatech
DEUTSCHE AKADEMIE DER
TECHNIKWISSENSCHAFTEN

Editor:
Prof. Dr. Dr. h.c. Johannes A. Buchmann
Technische Universität Darmstadt
Hochschulstraße 10
64289 Darmstadt
E-Mail: buchmann@cdc.informatik.tu-darmstadt.de

Recommended citation:
acatech (Ed.): *Internet Privacy. Options for adequate realisation* (acatech STUDY), Heidelberg et al.: Springer Verlag 2013.

ISSN: 2192-6174 / ISBN 978-3-642-37912-3 / ISBN 978-3-642-37913-0 (eBook)
DOI 10.1007/978-3-642-37913-0

Bibliographical information of the German National Library
The German National Library lists this publication in the German National Bibliography;
Detailed bibliographical information can be viewed at http://dnb.d-nb.de.

Springer Vieweg

Coordination: Dr. Karin-Irene Eiermann
Edited by: Jaina Hirai
Layout-Concept: acatech
Conversion and typesetting: Fraunhofer Institute for Intelligent Analysis and Information Systems IAIS, Sankt Augustin

Printed on acid-free paper
www.springer-vieweg.de

> THE acatech STUDY SERIES

This series comprises reports presenting the results of projects carried out by the National Academy of Science and Engineering. The studies are intended to provide informed assessments and future-oriented advice for policy-makers and society.

AUTHORS

- Prof. Dr. Dr. h.c. Johannes Buchmann, Technische Universität Darmstadt/CASED/acatech
- Prof. em. Dr. Rafael Capurro, formerly Hochschule der Medien (HdM), Stuttgart
- Prof. Dr. Martina Löw, Technische Universität Darmstadt
- Prof. Dr. Dr. h.c. Günter Müller, Albert-Ludwigs-Universität Freiburg
- Prof. Dr. Alexander Pretschner, Technische Universität München
- Prof. Dr. Alexander Roßnagel, Universität Kassel
- Prof. Dr. Michael Waidner, Technische Universität Darmstadt/Fraunhofer SIT/CASED
- Dr. Karin-Irene Eiermann, acatech office
- Dr. Michael Eldred, Cologne
- Florian Kelbert, Technische Universität München
- Daniel Nagel, Stuttgart
- Maxi Nebel, Universität Kassel
- Carsten Ochs, Technische Universität Darmstadt
- Martin Peters, Albert-Ludwigs-Universität Freiburg
- Dr. Philipp Richter, Universität Kassel
- Fatemeh Shirazi, Technische Universität Darmstadt
- Hervais Simo, Technische Universität Darmstadt

> CONTENTS

PROJECT

> PROJECT MANAGEMENT

Prof. Dr. Dr. h.c. Johannes Buchmann, Technische Universität Darmstadt/CASED/acatech

> PROJECT GROUP

- Prof. em. Dr. Rafael Capurro, formerly Hochschule der Medien (HdM), Stuttgart
- Prof. Dr. Martina Löw, Technische Universität Darmstadt
- Prof. Dr. Dr. h.c. Günter Müller, Albert-Ludwigs-Universität Freiburg
- Prof. Dr. Alexander Pretschner, Technische Universität München
- Prof. Dr. Alexander Roßnagel, Universität Kassel
- Prof. Dr. Michael Waidner, Technische Universität Darmstadt/Fraunhofer SIT/CASED
- Dr. Wieland Holfelder, Google Germany
- Dr. Göttrik Wewer, Deutsche Post DHL
- Michael Bültmann, Nokia GmbH
- Dirk Wittkopp, IBM Deutschland GmbH

> ASSIGNMENTS/STAFF

- Dr. Karin-Irene Eiermann, acatech
- Martin Peters, Albert-Ludwigs-Universität Freiburg
- Carsten Ochs, Technische Universität Darmstadt
- Fatemeh Shirazi, Technische Universität Darmstadt
- Hervais Simo, Technische Universität Darmstadt
- Florian Kelbert, Technische Universität München
- Maxi Nebel, Universität Kassel
- Dr. Philipp Richter, Universität Kassel
- Daniel Nagel, Stuttgart, Independent
- Dr. Michael Eldred, Cologne, Independent

> PROJECT COORDINATION

Dr. Karin-Irene Eiermann, acatech

> PROJECT PROCESS

07/2011 – 06/2013

> FUNDING

The project was financed by the Federal Ministry of Education and Research (support code 01/08/2011 – 30/09/2012: 01BY1175, 01/10/2012 – 31/01/2013: 16BY1175).

SPONSORED BY THE

Federal Ministry of Education and Research

Project administrator: 01/08/2011 - 30/09/2012: Project Management Agency – part of the German Aerospace Center (PT-DLR)

01/10/2012 - 31/01/2013: VDI/VDE Innovation + Technik GmbH

acatech would also like to thank the following companies for their support:

Google Germany, Deutsche Post AG, Nokia GmbH, IBM Deutschland GmbH

1 INTRODUCTION

1.1 SCOPE OF PROJECT

The present book is the second publication in a large-scale, interdisciplinary research project on Internet Privacy which was launched in mid-2011.The origin of the project is a condition frequently called the "privacy paradox". This paradox refers to the fact that people use the Internet extensively and often relinquish their data all too willingly, yet simultaneously harbor significant fears and worries – some justified, some exaggerated – that their privacy will be compromised. In short, we observe a coexistence of acceptance and fear with regard to Internet usage. This paradox may hinder the enormous potential of the Internet for users, businesses, and the economy, as users may be reluctant to use services that could benefit them significantly.

The goal of our interdisciplinary project was to develop recommendations (including technical prototypes) for policy makers and legislators, businesses, industry, researchers, and academia that promote a culture of privacy and inspire trust in Internet applications and online data transmission. These recommendations apply to the fields of education, business ethics, technology development, legal matters, and research demands. Following are proposed social rules and norms, a clear economic and legal framework, as well as technical solutions describing how an adequate measure of privacy can be evaluated and implemented in various Internet contexts. Web 2.0 (including social networks) and e-commerce are the primary focus areas.

These diverse requirements can best be fulfilled by an interdisciplinary approach that brings together expertise from various academic disciplines. Researchers from the fields of information ethics, sociology, law, economics, and technology contributed to the evaluation and structuring of our ideas, and the development of holistic options with wide-ranging application potential. Besides this academic input, the project group benefited immensely from the practical business perspectives of the Internet and communication companies involved.[1] The strategic decision to involve corporate players in the project enhanced the quality and practical reference points of the academic research and added relevance as discussions evolved around practical business cases.

We apply a normative, value-based approach to a culture of privacy and trust on the Internet. This value-based approach helps to structure the complex system of economic stakeholders, technical framework conditions, legal requirements and dynamic societal parameters that come together on the Internet and utilises the main pillars of a democratic society, including free individuals and economic well-being for all.

To reduce complexity and ensure thorough scientific examination, we limited the number of application fields. In the challenge to identify and select representative application areas for our options and recommendations, we were guided by an individual perspective and the question: what are people currently using? What are the sources of insecurities and legal disputes at the present time? We identified online social networks and e-commerce as the most widely used and therefore the digital spaces/areas most affected by insecurities and privacy concerns. Due to the near-universal nature of these two application areas and their successive convergence, we surmise that many conclusions drawn from them may be applicable for other relevant areas with potential for privacy violations, such as e-government and e-health.

1.2 GROUNDS FOR MULTIDISCIPLINARY ANALYSIS

As mentioned above, the project brought together various academic disciplines in the common pursuit of identifying the conditions for a culture of privacy and trust on the Internet. In the first phase of the project, the authors

[1] See list of participants in the preface of this volume.

saw a need to view privacy from various perspectives and juxtapose the different points of view and angles of reference. This way they are made explicit and valued as equally valid ways of looking at privacy. The desires and fears of users were studied empirically using social science methods. The ethicists provided a comprehensive overview of ethical and philosophical approaches to privacy and applied them to the cyberworld. There is also a detailed account of business privacy concerns online: as many services are paid for with user data, the question arose of what this means for the user. Another part of the study explored both the existing technical options to undermine privacy protection and those to enhance privacy protection (privacy-enhancing technologies, PETs). The final part examined the applicable legal framework surrounding data and privacy protection. The results of this analysis were published as Volume One of this project.[2] In order to give equal weight to each of the represented disciplines, the setup is an inherently multidisciplinary one, not an interdisciplinary joint endeavor.

1.3 INTERDISCIPLINARY SYNTHESIS

The formation of a culture of privacy and trust is a common task for all involved disciplines and actors and can only be realised through a synthesis of diverse perspectives. The present volume is characterized by a truly interdisciplinary approach. Based on the multidisciplinary analysis each researcher contributed his/her own particular approach to the applicable areas and the specific challenges to be addressed within those areas. The representatives of each discipline worked together to find a common denominator which allows for common acceptance of the proposed options. Looking at problems and application areas together, a synthesis of the disciplinary approaches is realised and executed through consideration and accommodation of the various discipline-based concerns and perspectives.

1.4 DESCRIPTION OF OUR APPROACH AND METHODOLOGY

In our efforts to develop options for improving privacy and trust on the Internet, we apply a normative and value-oriented approach. While interpreting privacy as a mode of social being, we do not regard privacy as a concept which has an intrinsic value. Rather, we consider privacy to be valuable and worthy of protection only insofar as it is crucial for the realisation, protection and improvement of selected values which provide the framework for our pluralistic democratic societies in Europe. We are anchored in a European value system, yet we believe that the values we have chosen – free self-determination, democratic participation, and economic well-being – have a broader appeal. They are an intrinsic part of universally accepted human rights and indispensible for a dignified life, free from hunger and from fear of oppression, violence, and injustice.[3]

1.5 STRUCTURE

This normative value-oriented approach predetermines the structure of our argument that is laid out in the present volume. We begin with a definition of the concept of privacy as we understand it and a description of three core values we have chosen as our framework. Chapter 2 concludes with an explanation of the way these three core values depend on the element of privacy for their realisation. In Chapter 3 and Chapter 4 we explore our application areas, online social networks (OSNs) and e-commerce, in great detail. Chapter 3 describes the stakeholders, the categories of data, the functions and implications of OSNs from a technical, sociological, ethical, and economic perspective and details the legal regulations which apply to this online area of application. Chapter 4 introduces the stakeholders and characterizes the transactions which occur in e-commerce. The technology behind e-commerce transactions, their social impact, ethical

2 Buchmann 2012.
3 General Assembly 2000.

issues concerning e-commerce and the legal environment are all described to gain a comprehensive, multi-perspective understanding of this complex area of online application. Both Chapter 3 and Chapter 4 also detail the benefits OSNs and e-commerce bring to the realisation of the core values.

Chapter 5 shows how these benefits may be impaired by threats and privacy risks which appear in the context of these two applications. First the authors introduce primary conditions for privacy protection and then go on to show in which ways these conditions – awareness, control, and trustworthiness – are threatened. In accordance with our overall line of reasoning the next step shows how these privacy threats undermine our three core values: free self-determination, democratic participation, and economic well-being. Finally in Chapter 6, the authors present a variety of options for achieving privacy in OSNs and e-commerce transactions. These options are divided into the categories of awareness, control, and trustworthiness, those conditions for privacy protection which were introduced in Chapter 5. Regulatory, technical, and educational measures as well as good practices to improve awareness, control, and trustworthiness are delineated.

In this volume we do not yet offer an evaluation of the options presented in Chapter 6. Rather, they are meant to showcase a wide range of possible measures that could be implemented for privacy protection. The actual evaluation of the options and subsequent deduction of recommendations for action for policy-makers and legislators, businesses, and civil society are published in a separate publication entitled acatech POSITION Internet Privacy.[4]

4 acatech 2013.

2 CORE VALUES AND THEIR RELATION TO PRIVACY

This chapter provides the basis for our overall goal of developing recommendations on how a culture of privacy and trust on the Internet can be fostered. We begin by presenting an understanding of privacy developed in the first stages of this project that is used throughout this document. Since the recommendations are derived from core values that we hold fundamental in our European democratic tradition and are also in line with an underlying understanding of human freedom, this chapter introduces the core values – free self-determination, democratic participation, and economic well-being – and indicates why we have selected them. Following this, we discuss each of the core values in greater detail, taking the perspectives of the social sciences, ethics and law into account. We also elaborate on the specific relationship between the core values and privacy. Showing the inextricable linkage between privacy and the basic principles of a free, pluralistic and democratic society will lay the foundation for transferring this relationship to the cyberworld,[5] and more specifically, to two exemplary Internet-application areas: OSNs and e-commerce.

2.1 PRIVACY

One definition we have found which takes into account a large number of relevant aspects was developed in the 1970s by social psychologist Irwin Altman, who conceptualized privacy as "an interpersonal boundary process by which a person or a group regulates interaction with others. By altering the degree of openness of the self to others, a hypothetical personal boundary is more or less receptive to social interaction with others. Privacy is, therefore, a dynamic process involving selective control over a self-boundary, either by an individual or a group."[6] Privacy for Altman is consequently in general an "interpersonal event, involving relationships among people."[7] According to his way of thinking, privacy norms are subject to society's definition, while individuals apply these norms within social situations, depending on the context as well as on the desired state of privacy they would like to achieve. In addition, drawing interaction boundaries regulates "Control of Input from Others" and "Control of Output to Others"[8] – in other words, the flow of information (outwards and inwards). In sum, Altman accounts for both the individual as well as collective dimension of privacy; he allows for the conception of privacy as a state of affairs to be achieved by various means: material (walls, clothes, technology), semiotic (signs) and normative (social rules and customs); and he is clear about the fact that while privacy might be related to information flow, it is generally about social situations.

If, however, personal privacy (in contradistinction to the privacy of private property[9]) is to be understood as a mode of social being, i.e. as a phenomenon relating to how human beings share the world with one another, Altman's definition must be examined closely, as an explicit phenomenological unfolding and subjected to critique.[10] Accordingly, personal privacy is fundamentally the aspect of social interplay relating to how persons show themselves as who they are, which includes the negative or deficient modes of such self-showing, namely, a privatio of self-revelation. Privacy thus consists of concealing who you are – either completely (anonymity, secrecy, incognito), or concealing only certain aspects of one's identity, (use of a pseudonym) or concealing identity only in certain situations and contexts (location and time). Privacy is multifaceted and complex, but all these facets relate to a person's identity through the various dimensions of self-display and self-concealment. In the Western world, personal privacy concerns an individual freedom of self-determining how to reveal oneself in

5 On the choice of the term 'cyberworld' in preference to 'cyberspace' Buchmann 2012, Sections 2.3.5 and 2.4.5.
6 Altman 1975, p. 6.
7 Altman 1975, p. 22.
8 Altman 1975, p. 29.
9 Buchmann 2012, Sections 2.2.5-2.2.6.
10 Buchmann 2012, Sections 2.2.1-2.2.5, 1.10 and 2.4.6-2.4.10.

the ongoing interplay of the social world. The interplay of identity formation is as much a freedom to display oneself as it is to withdraw and conceal oneself or to present oneself with a certain 'spin', i.e. self-display (showing off who you are) and self-concealment are two sides of the same, multifaceted coin. Furthermore, freedom pertains not to an actual state of affairs, but to a potential to determine one's own life-movements within the interplay with others, so it has the aspect of a social power play (that may also enter the political domain) which by no means guarantees a successful outcome. Hence, informational privacy, i.e. the freedom to self-determine what information (digital data) is released into or withheld from the public domain of the cyberworld, is merely derivative of the more fundamental individual freedom to play the game of showing oneself to others or concealing oneself from them in the abovementioned multifaceted sense.

We too, like Altman, conceive of privacy as a state of affairs being inherently social, that is, by "privacy" we mean a specific mode in which the social interplay is acted out. What follows from this is that privacy does not mean the isolation of an individual from the (social) world; rather, the concept refers to the specific and dynamic configuration of revealing and concealing who you are *within* the social interplay among the social players. However, while being subject to societal, customary definition, privacy preferences (i.e. what, how, how much, when and where an individual shows or conceals who he or she is) vary from one individual to another, so our understanding of privacy has to allow for a spectrum of individual privacy preferences. Secondly, whereas we are interested in *informational* privacy, we must always keep in mind that privacy is about social situations and people living their lives with one another. Therefore, we consider privacy a specific form of social interplay. And finally, here we do not leave the issue of whether to conceive of privacy as having some "intrinsic value".[11] Nor do we attempt to encompass all the phenomena falling under the rubric of privacy. Instead, in the present limited context, we treat privacy only insofar as it pertains to our chosen core values.

2.2 OUR APPROACH

Any presentation based on cultural values or basic social principles has normative features. Socio-cultural values arise from the desire to live well in a given society and assume the shape of norms and rules for human behaviour. Insofar as the selection of three core values we deem indispensable for a flourishing and free society – self-determination, democratic participation, and economic well-being – we follow a normative approach. One obvious reason for this is the value-context in which this text is produced. We believe that value-orientation is a vital precondition for any culture of privacy and trust, both in the offline world and in the cyberworld. We are well aware that a normative approach is culturally specific and is indebted to the ideal of a European community of values. We are also aware that this ideal has been thoroughly deconstructed.[12] Whereas such deconstruction may modify our understanding of these values in the sense that they become visible as a culturally-generated ideal, this consideration does not lead to a repudiation of these values. As the values cherished by Europeans correspond to a deeper understanding of freedom whose validity is upheld interculturally, our approach is open to a dialogue between all those committed to human freedom per se, albeit in various cultural guises.[13] An approach based on considerations of human freedom *per* se is no longer normative (since freedom is an option for living together, not a moral imperative), but sheds light on how human beings can freely share a world.

11 To do so would be to follow here Daniel J. Solove, who holds that "The value of ameliorating privacy problems lies in the activities that privacy protections enable." Solove 2008, p.85. However, against this argument from consequences, it must be kept in mind that the social interplay of revealing and concealing who you are is a core aspect of freedom *per* se that cannot be traded off for functional benefits or consequences.

12 Chakrabarty 2007.

13 Buchmann 2012, Section 2.5.

Within this value framework, our three selected core values: free self-determination, democratic participation and economic well-being, relate intimately with human freedom. Free self-determination is a precondition for fostering free, self-determined and responsible individuals constituting a free society. Democratic participation, a value guaranteed on the political plane by the German constitution, ensures the sovereignty of the people and is also a precondition for a free democratic society. Economic well-being is a basic goal of a free market economy where cutthroat or unfair competition among the players is suppressed for the sake of the freedom and fairness of interplay. Good governance needs not only to ensure basic economic well-being for the people in the sense of a standard of living, but also to secure the framework within which economic players can freely and fairly engage in pursuing a livelihood.

When elaborating upon these values of freedom, our ultimate objective is to deliver a richer view of each value by bringing together multiple perspectives into a multifaceted, inclusive description. Such a comprehensive depiction of the various dimensions of a core value is necessary to assess an Internet application's potential for enhancing and promoting that value whilst at the same time identifying possible risks and threats to it, tasks we take on in Chapters 4 and 5. We integrate sociological, ethical, legal, economic and technical perspectives to pinpoint opportunities as well as potential threats for both individuals and society as a whole (sociological and ethical), for users and consumers (economic), and the respective constitutional rights (e.g. the right to informational self-determination) and national objectives e.g. democracy (legal). Technological solutions and limitations provide boundaries for proposals as to how our values can be manifested in the cyberworld.

A multi-perspective approach leads to uncovering viable options from the opportunities and risk-scenarios identified. A multidisciplinary perspective is also helpful for establishing context when evaluating threats to a given core value, where a seemingly harmless deviation in one context can have detrimental consequences in another. We now proceed by elaborating each of our core values and exploring how privacy as outlined above relates to each one of them.

2.3 FREE SELF-DETERMINATION

Free self-determination lies at the core of any understanding of freedom because ultimately each individual human being controls his/her own life-movements, even when they submit freely or under compulsion to another, whether it be another person, an institution such as the state, or the tenets of a religion. Free self-determination also lays the foundation for creating a singular identity. Identity-formation, in turn, is the interplay with the world through which a who[14] finds its self reflected by the world, thus casting and assuming its self-identity.[15] One's identity goes hand in hand with revealing and concealing who one is and is already shaped within the rules of interplay of a concrete culture within a shared world. A self has to be free to shape its own life and to freely express its decisions in an interplay with other self-determining selves if true freedom is to be achieved. The free – invariably courageous – existential shaping of one's own life also pushes the boundaries of how others can shape their own identities in the shared world by showing alternative socio-cultural options for identity formation, which historically are constantly in flux. In this sense, self-determination cannot be restricted to individual aspects of life (individualism), but colours and influences the freedom of social interplay as a whole, and not only within the European context.

14 The distinction between *what* and *who* is essential; Buchmann 2012, Section 2.2.1. Cf. also "While literature on the 'digital identity' is growing, newer research has shown that it is not enough to analyse identity questions in terms of those matters that mostly concern the *identification of a person* rather than his or her *identity as a person* (philosophy distinguishes between identity of the same – idem – and identity of the self – ipse)." EGE 2012, p. 38.

15 Buchmann 2012, Section 2.2.2.

2.4 PRIVACY IN RELATION TO FREE SELF-DETERMINATION

Free self-determination is dependent on both intrinsic and extrinsic factors. It requires a self capable of presentation within the interplay with others, and thus also able and willing to risk participating in the play of concealment and disclosure.[16] However, free self-determination concurrently implies a self freely able to cast its identity within the implicit and explicit rules of interplay in a given society. A free society thus provides a framework within which such choices of the self are both safeguarded and catalysed, including how this self can present in different contexts, both revealing and concealing certain facets of the self. The tension between free self-determination and the interests of others or the state is mirrored in privacy debates when, for instance, privacy is restricted for security reasons.[17] However, it has to be kept in mind that free self-determination also benefits society by enabling and fostering creative, courageous citizens. Free self-determination as central to any kind of human freedom goes hand in hand with privacy since the individual freedom to reveal and conceal – i.e. to pretend to be, in the broadest sense, who you are – is an essential aspect of free, self-determined life-movements.

A major safeguard of freedom is privacy in the restricted sense of being able to withdraw certain aspects of the self from (public) disclosure into concealment. Self-presentation has self-concealment as its inverse. If privacy is not guaranteed as a retreat from the shared world, the self is deprived of necessary physical, psychological, spiritual and emotional preconditions for the reflection and evaluation that enable free formation of identity. Privacy, however, is not synonymous with the private sphere, but also encompasses the freedom of self-presentation in public whilst maintaining concealment of other aspects of one's self, i.e. there is an inherent tyranny in demanding that any self should totally reveal who they are, and in many contexts anonymity must be safeguarded in public intercourse such as commerce.

However, safeguarding privacy cannot be simply decreed. A single all-encompassing 'right to privacy' is not granted in the European context. While Art. 7 of the Charter of Fundamental Rights of the European Union (CFREU) guarantees an abstract respect for private life,[18] Art. 8 CFREU is more specific in protecting personal data. In Germany, the complex of privacy can only be described legally via the interplay among several basic rights accorded to individuals and the public interest. With regard to privacy on the Internet, the basic right to informational self-determination in Arts. 2.1[19] and 1.1[20] Grundgesetz (GG, the German constitution) is the most prominent, from which systematically follow all German data protection regulations. The EU Data Protection Directive[21] does not mention informational self-determination explicitly, but the EU data protection acts are all heavily influenced by this German basic right and the associated jurisprudence. Informational self-determination is not a "right to be left alone in isolation", but rather the individual's right to monitor personal information in the process of communication with others. This concept is in accord with Altman's privacy definition, but misses the basic distinction between the *what* of information and the *who* of free selves living their self-determined lives, both showing and concealing who they are. Indeed, without having the who behind the what of digital data

16 Buchmann 2012, Section 2.2.4.

17 Solove 2011.

18 International Covenant on Civil and Political Rights (ICCPR), Art. 17; Universal Declaration of Human Rights by the United Nations (UDHR), Art. 12; European Convention on Human Rights (ECHR), Art. 8.

19 Art. 2 (1) GG: Jeder hat das Recht auf die freie Entfaltung seiner Persönlichkeit, soweit er nicht die Rechte anderer verletzt und nicht gegen die verfassungsmäßige Ordnung oder das Sittengesetz verstößt.

20 Art. 1 (1) GG: Die Würde des Menschen ist unantastbar. Sie zu achten und zu schützen ist Verpflichtung aller staatlichen Gewalt.

21 EU Directive 95/46/EC.

circulating in the cyberworld, it is impossible to distinguish between data needing privacy-protection and data that is innocuous. Thus, if the principle of self-determination over personal data were applied in a blanket manner, the cyberworld itself would become impossible, because every single movement of an individual in the cyberworld necessarily leaves behind a digital trace whose informational release would require personal consent. This is not a trivial detail. Furthermore, privacy cannot be protected without an active involvement of the self, as only the self is able to determine the boundaries and play of personal concealment and also subtle modes of disclosure. Conversely, society must also be taken into account, since personal preferences might lead to a level of self-concealment detrimental to other aspects of sharing a social world. In certain contexts it is imperative that a self reveals who they are for the sake of public order, e.g. when boarding a flight at an airport or when an income-earner is compelled to assume the identity of a taxation file number.

2.5 DEMOCRATIC PARTICIPATION

Democratic participation, here viewed far more broadly than the people's right to participate in free and fair elections to elect a government, is a core characteristic of personal freedom. Namely, it encompasses everyone's freedom of self-presentation in the form of (public) self-expression and thus the freedom to participate in social goings-on and to have one's say, including in elections.[22] Such expressive freedom cannot be lived by distancing oneself from others and the world, but only by taking a dynamic stance in the interplay with others in our shared world. Freedom of expression, political and otherwise, is one essential facet of the freedom of individual life-movements. Participation in public power plays at all levels safeguards the fluidity of interplay, freeing it from overly-restrictive rules and customs by addressing and challenging them via e.g. art or the full gamut of critical discourses. Democratic participation is also a guardian of personal autonomy. A self cannot be truly autonomous in the sense of being self-determined unless it also participates critically in the ongoing social dialogue in an interplay with other self-determining selves that contributes to shaping what existential options a given society offers.

2.6 PRIVACY IN RELATION TO DEMOCRATIC PARTICIPATION

To what extent can democratic participation benefit from and tolerate privacy and how do they interact and depend on each other? If privacy is a privatio in the sense of concealing certain aspects of the self from public disclosure, then democratic participation, understood as free and fair social interplay, requires that such personal privacy be safeguarded. A stock example is the secret ballot essential to free and fair elections. Personal privacy guarantees the freedom of choice, that is, the choice whether certain opinions, facts, and facets of a self's personal world and self-presentation to the world are disclosed or concealed, and within which circle of openness, broad or narrow. However, privacy is also a necessary condition for democratic participation insofar as privacy establishes the zones and contexts that make selectively negotiating the social rules of interplay and citizens' relation to the state possible in the first place: privacy allows for "limited and protected communication".[23] It safeguards the opportunity for group members to share their worldviews, exchange religious or other sensitive/private views, and to engage in debate in self-selected contexts. The self you present in various contexts, including what you say when and where and to whom, is an essential aspect of modulating and self-determining your own democratic participation in society. In this sense, not only informational privacy, but the personal freedom both to express and show one's self and to refrain from such self-disclosure, contributes to democratically shaping the political will.

22 Buchmann 2012, Section 2.4.4.
23 Westin 1967, p. 32.

As for the sovereignty of the people who take part in the political formation of will and decision-making processes through public debate, it is vital for every citizen to be able to engage in free speech and to assemble freely as their statutory right without fear of repression. Conversely, if verbal expressions become public beyond the chosen context, individuals might be deterred from speaking freely. Likewise, these individuals might be deterred from taking part in assemblies if everyone were able to learn that they had attended. Privacy at certain times or locations is necessary not only for people to participate, but also to be able to participate *without coercion*. Such legally-sanctioned concealment, i.e. privacy, safeguards self-determined democratic participation. It may also be important for some people to keep private (secret) party, club or union memberships, to engage in such activities without unfair social pressure. Privacy is consequently a vital aspect of democratic participation.

2.7 ECONOMIC WELL-BEING

Economic well-being in a (reified) market economy mediated by commodities is equated with earning a livelihood. Earned income is spent on those commodity services and products of all kinds that contribute to living well in a material sense. From this way of life arise the needs that can be satisfied by consumers spending income.[24] Income is gained through partaking in the gainful game[25] with other players (who include the collective enterprise players striving to earn profit-income). This game is played by competing for income within the constantly fluctuating, estimating interplay among economic players mediated by things of value. Any positive individual outcome of the gainful game thus represents a livelihood earned for the player concerned, along with the player's dependants. For a whole economy, well-being in one sense amounts to flourishing income-earning for all involved. In another sense, however, economic well-being resides in the freedom and fairness of how the gainful game is played out in striving for potential gain. The competition for income in the gainful game of a market economy should be fair; anything else is an abuse of social power. Such fairness is endangered, in particular, if any of the players is able to secure any, sometimes subtle or hidden, kind of monopoly, whether it be on the side of the employers, the enterprises, the financiers or the landowners.[26] (An interventionist economy may have also state enterprises, including such that are state monopolies.) For employees, in particular, who earn wages and salaries as income, economic well-being consists not only in earning enough, but also in having one's abilities fairly estimated and valued by the market (usually the particular employer). All income earners as consumers have an interest in being able to procure goods and services supporting a good life at reasonable prices, i.e. prices undistorted by any kind of monopolistic or other unfair trade practices. Freedom is served only when the economic interplay of the gainful game is fair and not unnecessarily hindered.

2.8 PRIVACY IN RELATION TO ECONOMIC WELL-BEING

We have seen that privacy is indispensable for realizing the core values of free self-determination and democratic participation. Regarding the third core value, economic well-being, however, things are not as clear-cut. On the contrary, in the context of today's emerging cyberworld, privacy requirements are typically perceived as a threat to economic well-being. In this section we examine to what extent this may be the case. Data-centric business models incorporating the necessity of achieving economies of scale may generate temporary monopolies. A revised and adapted understanding of privacy, at first glance apparently unrelated to information asymmetries, may be a means of enabling a sustainable equal power distribution amongst the stakeholders, which may indirectly influence economic well-being.

24 Buchmann 2012 Section 2.2.11.
25 Buchmann 2012, Section 2.2.6.
26 ibid.

We contend that companies may have difficulties and ultimately may be forced out of business if they face very strict regulation in terms of data-protection guidelines. The economic players most affected by privacy regulations, and accordingly a focus of our study, are data-centric services. Data-centric services offer seemingly free services (that cost something, perhaps a great deal of money, to provide) in exchange for personal data. While users pay a certain 'price' (their personal data, as yet unmonetised) for a certain service or good, the data-centric service determines another (realised monetary) price to be paid by third parties (such as advertising agencies) with an interest in the personal data originally provided by the users of the data-centric service. Perhaps such a business model per se violates a well-considered concept of freedom.

Negative impacts of privacy on data-centric services

Several factors may make the provision of data-centric services more expensive, thereby reducing the profits of the companies offering these services. If a business model is based on the sale of personal data gathered from customers, who in exchange receive cheap or free goods or services, that business model will be compromised and services reduced if data-protection regulations prohibit personal data from being processed and passed on in any form. The same is true if legal regulations require anonymization of data which makes them less valuable for the mining of commercially pertinent information. Furthermore, acquiring privacy-enhancing technologies (PETs) can be an expensive investment for private companies. If data-protection restrictions are imposed only on some companies by national legislation they may face a distinct disadvantage *vis-à-vis* their transnational competitors who are not subject to these restrictions.

Another consideration is that if companies do not take measures to protect (informational) privacy, this may have to be done by the state. The legislator may be reluctant to impose privacy regulations on private businesses for the reasons stated, yet may still deem it necessary to implement privacy measures. This represents a burden on certain enterprises and indirectly on the state budget and taxpayers, insofar as the economy generates less total income and hence a smaller tax-base. This way of arguing basically from the viewpoint of benefits, efficiency and effectiveness, of course, points to economic consequences and results, whether they be benefits or disadvantages, either for certain economic players or for the whole economy or the state, thus pushing aside considerations of the intrinsic (non-economic) value of privacy as an essential aspect of personal freedom, which in the first place is a potential, not an actuality. To see this, one must step back from a narrow view of privacy as informational data privacy and the potential monetization of private data. From this perspective, the freedom to reveal or conceal who you are in various contexts is not negotiable for the sake of economic benefits, whether they be enhanced income generation or lower prices for some or for all. Furthermore, there is a fundamental flaw in regarding economic well-being as residing solely in the income actually generated by individuals, sectors or the economy as a whole since the gainful game is also a way of life borne by the actions of players whose freedom consists of the potential promised by the striving for income, i.e. "the pursuit of happiness", and not in guarantees of secured success. In this latter sense, economic well-being amounts to a free and fair gainful game.

Positive impacts of privacy on data-centric services

Leaving these considerations aside, however, recent empirical studies have shown that protecting customers' privacy also can have a positive impact on income generation and corporate profits, in particular. One aspect in this regard is the economic paradigm that information asymmetries due to a lack of data-privacy have negative impact on the economy in terms of their actual results. The other aspect is the enhanced reputation of a company consumers trust because they feel secure in entrusting their data to it without the fear of inappropriate use in other contexts.

Regarding the first aspect, economics Nobel laureate Joseph E. Stiglitz and his team have shown that information asymmetries lead to asymmetries in market economic power, i.e. unfairness in the gainful game, and thus cause economic problems.[27] Asymmetry means that certain parties have an information deficit and therefore are at an unfair disadvantage in the market interplay. Information asymmetries are present when there is insufficient transparency for customers about how their personal data is used and, accordingly, what their personal data is worth for a given data-centric service. The latter may use personal data for new transactions which lead back to the consumers even if they may not know of the existence and use of aggregated information. Our elaborated understanding of privacy implies that an important aspect of privacy is informational self-determination. Typically, a lack of informational self-determination starts with an information deficit on the part of the user. As a result, the user cannot control the use of his or her information. According to Stiglitz' theory, this information deficit may have detrimental effects on overall income generation, which implies that strengthening privacy may be a requirement for economic well-being conceived as *actually* achieved income-generation. Information deficits based on a lack of informational privacy presumably accelerate economies of scale and increase consumer/user switching-costs, which may have positive short-term impact on economic output and individual productivity, but in the long run may lead to monopolisation and thus threaten economic well-being conceived as free and fair economic interplay Therefore, we can expect that strengthened informational self-determination might reduce the risks of said information deficits occurring.

The second aspect comes into play when a product becomes more valuable for the consumer because of additional features. This is the case if the producer or seller of that product behaves in a privacy-friendly manner. As users become aware of their privacy requirements, privacy-friendliness can become a valued feature of data-centric services that may turn out to be a competitive advantage. Recent efforts by companies such as Google (with Google+) and Facebook to add privacy features and create more transparency for users show the importance companies are beginning to assign to privacy, or rather the relevance of privacy in users' or customers' decision-making. In a contested market environment, privacy-friendliness provides a competitive edge and customers have shown a willingness to pay for the privacy of their personal data. Studies suggest that overall, the importance of privacy for the exchange of products and services is dependent upon their sophistication, i.e. usually consumers of high-end products and services tend to invest more in privacy than buyers of low-end products.[28]

27 Akerlof 1970, pp. 488–500.
28 Turow et al. 2005, p. 25.

3 THE CHARACTERISTICS AND BENEFITS OF ONLINE SOCIAL NETWORKS

This chapter characterizes today's online social networks (OSNs) and develops an interdisciplinary understanding of them. To this end, each discipline characterizes OSNs from its viewpoint, thus using different foci and laying the foundations for a common understanding. We conclude this chapter with a shared interdisciplinary view of OSNs by pointing out the similarities between the different viewpoints.

Borrowing from boyd and Ellison, we define "social network sites as web-based services that allow individuals to (1) construct a public or semi-public profile within a bounded system, (2) articulate a list of other users with whom they share a connection, (3) view and traverse their list of connections and those made by others within the system",[29] and (4) allow users to communicate over the Internet as well as to share interests, media, and activities, often via third-party applications.

3.1 TECHNICAL PERSPECTIVE

From a technical point of view we focus on two major parameters that characterize OSNs: the stakeholders involved and the various types of data, including their collection and usage. We conclude by offering our thoughts on the function of OSNs as the new desktop.

3.1.1 OSN STAKEHOLDERS

Users

OSNs such as Facebook, Google+ and others are experiencing tremendous growth with millions of active users every day. A social network user is any legal entity, i.e., an individual or organisation, that subscribed to the OSN service and hence is associated with an online profile. Passive users, in contrast, have not subscribed to the service but may still be using (knowingly or unknowingly) public services of the OSN.

OSN users have the ability not only to create and manage their respective profiles, but also to create and manage relationships with other users based on common interests, such as entertainment, social events, or professional issues. This way, users sharing similar interests or social relationships in the physical world can build communities in the cyberworld. Social network users can browse through their contacts' profiles and contact lists, upload multimedia content, post private and/or public messages, and annotate (user-generated) content with reviews, comments, and recommendations.

Social network operators

Operators provide the underlying basic services, e.g. access to the networking site and to social plug-ins, and infrastructures, e.g. servers for storing and sharing various types of user-related data, needed by users to interact with each other. To make their platform attractive, most operators define Application Programming Interfaces (APIs) which third parties can leverage to deploy additional services. Organisations and other entities can rely on those interfaces to make their entire online platform social, thus extending their services without having to operate their own social networks. Indeed, traditional websites are increasingly partnering and interfacing with social networking services to offer their visitors a personalized and social Web experience. This adoption of online social networks has led to enormous amounts of sensitive personal data being entrusted to social network operators. Furthermore, since the monetization of OSN-entrusted data is becoming the foundation of online business, operators typically rely on the graph API to share information about users (e.g., attributes, activities, interests, and their relationships) with advertisers[30,31] application

[29] boyd/Ellison2007.
[30] Rohan et al. 2008.
[31] McCarthy 2010.

developers[32,33] and other third parties[34,35] Section 3.3 will explain the operators' business models in detail.

Third parties

Third parties are individuals or organisations providing applications, services, and functionalities other than those already provided by the social network operator. Third parties interact with the social network without being part of it. They rely on the APIs defined by the social network operator to develop and deploy applications and services (e.g. games, music-sharing, personalized advertising). To deliver attractive features, these applications and services are typically designed in a way that allows them to gain access to user information (identity attributes, contact details, posts, browsing history, etc.). There are various types of third parties, including advertising agencies, researchers eager to study similarities between user behaviour in the cyberworld and typical behaviour in physical environments; government agencies that are increasingly interested in monitoring OSNs with a view to preventing social disorder and crime, and data aggregators who gather details about user profiles and activities from various social networks in a single domain.

Internet Service Providers

An Internet Service Provider (ISP) is the corporate entity that mediates between the social network platform, users, and third parties by providing the medium through which bit-strings, and thus information of all kinds, are passed. ISPs thus form the physical backbone of the cyberworld. As an intermediary between all other stakeholders, ISPs have the potential to monitor and collect information about users' communication and activities on the social network. In some countries, ISPs are required by law to collect and retain customer transaction data such as source, destination, type, date, time, and duration of communication. The period of retention in Europe is at least six months.[36]

3.1.2 SOCIAL NETWORKING DATA

When participating in OSNs, users disclose a variety of personal data, either deliberately or unwittingly. User-related social networking data includes:

- Identity data. Describes who the user is in the social network and includes identity and profile attributes as well as personal privacy settings.
- Content data. All content generated and/or uploaded by OSN users, e.g., messages, photos, videos, posts, comments.
- Social-graph data. Tracks which user knows which other users to which degree and how they are linked in the social network. They include social and trust relationship details.
- History and traffic data. Refers to what the operator may collect about users' interactions and activities relating to their use of the OSN. They typically include the users' browsing histories along with other details such as commented topics, visited profiles, location (e.g., IP address or GPS data), frequency and duration of use of certain services.
- Inferred data. All data that a social network operator or third party has inferred from collected data, therefore creating new information by, for example, combining the data of different users (or user groups). Such data includes recommendations (e.g., for contacts, services, games, music) and statistical information.

3.1.3 DATA COLLECTION AND USAGE

In most cases both the OSN provider and third parties finance their services by monetizing users' data. The collection of data can be classified into user-aware and user-non-aware (inadvertent) data collection. Naturally, this distinction varies

32 Facebook 2013.
33 Google 2012.
34 Facebook 2011.
35 Google 2012.
36 EU Directive 06/24/EC.

from user to user. Most users are aware that identity data and content data are collected and utilised. In the case of non-native services, i.e., services provided by third parties, users have to give their consent to let these third parties access certain information. However, users are frequently unaware of exactly which data is collected and whether it is permanently stored or further disseminated. Most users are also not aware that providers collect additional information about their behaviour, surfing history, and preferences. Such data may (transparently for the user) be collected using cookies, the Like/+1-Button, server-side logging mechanisms, etc.

After collection, operators and third parties use the data to generate revenue for purposes of financing (e.g., to pay infrastructure and stock owners), as well as improving and personalizing their services. The data may either be used on a per user basis for personalization, or on the basis of user groups, employing data-mining technologies to systematically extract useful, previously unknown information. Social search, personalized advertising and Web pages are probably the most well-known examples of the former. Using data mining, companies may detect new trends, markets, or users' desires at an early stage. Some technologies, such as recommendation services, even combine the two approaches.

3.1.4 OSNs AS THE NEW DESKTOP

Today's OSNs are realised as web platforms providing subscribed users the ability to connect and share information with other users in various forms, partially replacing communication services such as email and telephone. By offering APIs, OSNs are highly flexible and make it easy for third parties to integrate any kind of non-native web service (e.g., games, email, music) into the platform. As more and more services are integrated, OSNs may become the single point of entry to the Internet, providing various services through a single interface.

This development has been made possible through (1) the dissemination and easy usability of personal computers, (2) maturity of the Internet infrastructure (high availability, reliability, and performance), (3) Web standards allowing for highly interactive cross-platform Web services (Web 2.0), and (4) low entry barriers to Web services (no installation and configuration). The combination of these factors has led to high Internet usage, the emergence of OSNs, and users subscribing to these social and entertaining Web services.

3.2 SOCIAL-SCIENTIFIC AND ETHICAL PERSPECTIVE

In this section, we will characterize the quality and different forms of sociality OSNs help to develop. First, we will provide an abstract description of the social interactions OSNs make possible. Second, we will determine which groups make use of OSNs for what purpose, and what kinds of social relations are concerned. As presenting all possible uses for OSNs is downright impossible, we concentrate on the most prevalent ones.

3.2.1 SOCIAL INTERACTIONS

The social interactions observable on OSNs can be understood as the interplay of revealing and concealing between self-determining selves. This interplay shapes both society and individuals. Selves are only able to show who they are and to try them-selves out in interplay with others. OSNs have taken this interplay to a broader, digital stage. The self is no longer restricted to the social surroundings of his/her offline world, but is able to engage and disengage in other kinds of interplay at the same time through the medium of the cyberworld. Paradoxically, the cyberworld offers more options for such interplay, while simultaneously limiting the closeness of the encounter.[37] Nevertheless, with the advent of the cyberworld, the possibilities for revealing who one is have greatly multiplied. OSNs are probably the most prominent example.

[37] Bodily human presence is exchanged for bit-streams of data generated by a materially outsourced, calculating human logos of an arithmetic, algorithmic nature.

They simultaneously enable and enhance the showing-off of a self and facilitate pretending to be who one is through the adoption of one mask rather than another, as the other players in the game of self-presentation only get to know this self via the bit-streams of available data, that is, unless there is also an opportunity for a physical encounter.

3.2.2 USER GROUPS AND PURPOSES

When it comes to the user groups using OSNs, their motives for doing so, and the forms of sociality established via OSNs, it makes sense to start with an analytic distinction: usage that is related to individual users' life-world and usage that is observable in more formal, e.g. job-related, contexts. Since the former is the most prevalent, and also the most widely discussed, this is where we begin.

Private usage

The first observation to be accounted for is that, while the overwhelming majority of OSN users are young people,[38] their major motivation is to maintain social relationships generated in the offline-world[39] Using OSNs is therefore not so much about extending, but about *maintaining* one's social network: even if many users increase the number of their virtual relationships, the core network usually consists of only seven to ten people[40]. Furthermore, using OSNs is associated with accumulating three different types of social capital: (1) "bonding social capital", close relationships that offer all types of support, including emotional; (2) "bridging social capital", the infamous "weak ties" who might provide useful information and new perspectives; and (3) "maintained social capital" that allows actors to keep in touch with social networks after physically disconnecting[41] from them . Qualitative research shows that actors make use of OSNs in order to position themselves in their social networks. They practice "impression management", thereby learning to act socially and to negotiate the rules of sociality[42]. As users under the age of 25 report that they genuinely have no choice when it comes to using OSNs, it is plausible to diagnose significant peer group pressure to share the OSN experience: non-usage is associated with the threat of being cut off from real world networks.[43] In

38 98% of German people under the age of 30 are online (DIVSI 2012, p. 15). While 94% of the 14- to 29-year olds make active use of OSNs, only 76% of the 30- to 49-year olds do so (and for people 50-plus the percentage is 47%). Regarding Facebook, the OSN most heavily used, it is used by 72% of the 14- to 29-year olds, and only 38% of the 30- to 49-year olds (BITKOM 2011, pp. 4-5). Another 2011 survey generates the same figures for Facebook use of Internet users at the age of 12 – 19 years (72%) (JIM 2011, p. 48).

39 The fact has been empirically well-established that the major motivation for using OSNs is to cultivate relationships, which is confirmed by all the recent studies concerning the matter. The aforementioned DIVSI-study, for example, identifies as major motivations: "stay in contact with friends" (90%), followed by "chatting" (59%), "knowing what's going on" (53%) and "being informed about upcoming events" (42%). The motivation "finding new friends" ranks fifth (38%), while more specific activities, such as uploading and commenting on photos or videos, and sharing links and the like are only pursued by about one fifth (or even less) of the interviewees (DIVSI 2012, p. 53). A similar picture emerges from the BITKOM-study concerning OSN-usage: as far as "positive experiences" made on OSNs are concerned, cultivating friendships ranks highest (88% of 14-29 year olds), followed by "being informed about or invited to events and meetings" (73% of 14-29 year olds; see BITKOM 2011, p. 9). Likewise, the 2011 JIM-study identifies "chatting" and "sending messages to others" as major activities on OSNs (JIM 2011, p. 49). We can therefore conclude that OSNs are mainly used to cultivate pre-existing relationships by communicating synchronously (chat) or asynchronously (sending messages, sharing information about real life events), with secondary activities (e.g. uploading photos) serving as rather specific techniques assisting in the process of maintaining and organizing sociality.

40 Whereas the number of OSN-contacts ("friends") an average user has is between 120 and 130, with young users usually having more, i.e. about 200 contacts (BITKOM 2011, p. 12; JIM 2011, p. 49) Facebook chief social scientist Cameron Marlow states that "an average man – one with 120 friends – generally responds to the postings of only seven of those friends by leaving comments on the posting individual's photos, status messages, or wall. An average woman is slightly more sociable, responding to ten." (Wang et al. 2011, p. 11).

41 Ellison et al. 2007.

42 boyd 2007.

43 Again, the numbers are telling: if, practically speaking, the whole youth population is online (98 %, see DIVSI 2012, p. 15), and if 94% of those users are active on OSNs – most of them on Facebook (BITKOM 2011, pp. 4-5) – this leaves little choice for individual users if they want to partake in the interplay of revealing and concealing between selves. We furthermore gained insights into the peer group pressure issue in our own focus groups; ethnographic evidence is provided in Raynes-Goldie 2010.

this sense, the processes occurring on OSNs constitute society as much as any face-to-face interaction.

Some scholars hold that the success of OSNs indicates a shift in the way online communities are organised: increasingly around people, not interests[44]. As they are organised around people, for OSNs to become attractive it is crucial that they offer a range of multimedia applications (games, rankings etc.) and communicative channels (chat, public post, private mail). Also, it is a widely held and plausible social scientific assumption that the exchange of gifts indeed constitutes relationships, as it induces a mandatory kind of reciprocity[45]. Consequently, features that allow for "sharing" content (music, videos) can be considered particularly effective for establishing and maintaining OSN relationships. Facebook, for example, has a manifold of the mentioned features on offer. In addition, it started out as a tool to organise geographically-bound real world communities (college populations). As OSNs are most frequently used to organise offline relationships, its success might be due – at least in the Facebook case – to its capacity to bring offline social networks online, using the techniques mentioned above.

Professional usage

When it comes to more formal uses, OSNs have become similarly indispensable: having no account on a business platform (such as Xing), in some areas, might create real disadvantages when applying for a job. The type of social capital generated by using these platforms is mainly bridging and maintained social capital. In case of closed OSNs that are increasingly integrated into companies' every-day work practices, OSNs assist in organizing the offline-network and the workflow by offering communication tools and features allowing for sorting and displaying information. Another business-related usage pattern concerns the creation of customer ties on (thematically unspecified) OSNs. Here, the purpose is to tie the customer to some brand, and to gain personal information concerning the user's likes and dislikes, and usage patterns in order to gain the possibility of micro-targeting. A similar marketing purpose is to be found in the context of political parties.[46]

The fact that there are many companies and parties doing marketing on platforms such as Facebook illustrates that life-world usage and formal usage, while being distinguishable analytically, empirically tend to merge more and more. Users are targeted by companies when spending time with their peers on OSNs; employees increasingly make personal use of OSNs when at work.[47] Thus, OSNs and their uses, while playing an ever-increasing, integral role in constituting sociality, at the same time have the intrinsic capacity to break down social barriers we used to take for granted.

3.3 ECONOMIC PERSPECTIVE

From an economic point of view, OSNs are intermediaries connecting users and advertisers through their platform. We focus on two parameters that need to be considered: the way personal data is used for marketing and how the economic efficiency of these various possibilities is measured

3.3.1 MARKETING VARIANTS FOR PERSONAL DATA

The business model of any OSN is to offer free or subsidized services in exchange for the collection of personal data. These personal data are then marketed in three variants: as direct advertising, as skimming consumer surplus, and as inferences.

---

44 boyd et al. 2007.
45 Mauss 1968.
46 Siri et al. 2012.
47 For two and a half hours per week, 1 in 4 employees is active on Facebook for personal purposes while being at work. The time spent non-working amounts to 26,8 billion Euro – although we do not know if people who spend their time on Facebook now would otherwise simply be smoking, drinking coffee, having a chat or the like. YouCom 2011, p. 2.

- Direct advertising: OSNs are intermediaries connecting consumers and advertisers. OSNs do not provide personal data to the advertisers. Nevertheless, economically they fulfill the need of many companies to "know their customers" better than any other form of advertising. For dual-valued transactions OSNs play the role of a mediator and provide a platform where advertisers and customers meet. Different business models of OSNs have their specific emphasis on personalized vs. untargeted advertising. However, personalized advertising is the driving factor of the development from e-commerce to social commerce.
- Skimming consumer surplus is the tailoring of offerings by the provider based upon an understanding of the price a consumer is willing to pay for a given product. Auctions and reverse pricing as well as consumer profiling reduce consumer surplus.
- Inferences are drawn from collected data about behaviour and usage patterns. The correlations with other events constitute a new source of income resulting in added value for the provider. This is due to the revelation of implicit preferences inferred from available consumer data.

3.3.2 MEASURES OF ECONOMIC EFFECTIVENESS

These sources of income are not mutually exclusive and depend upon the analytic capabilities of the OSN. Analytics are applied to increase effectiveness with regard to ad impressions, brand awareness, and conversion rates. In terms of accuracy and coverage OSNs are more attractive to advertisers than classical methods of information collection and provision like market research, print, and other offline media. Effectiveness is usually measured in cost-per-click (CPC), cost-per-action (CPA), and cost-per-order (CPO). Only clicked ad impressions (CPC), downloaded files (CPA), and sold products (CPO), count as advertising success for which advertisers have to pay. In contrast to reachability-oriented revenue models such as thousand-ad-impressions (TPI), where prizes are calculated according to the amount of money required to attract the attention of thousand visitors, performance-oriented models are more effective for targeting. A recent study by Microsoft, United Internet, and Yahoo shows that performance-oriented online advertisement outperforms reachability-oriented TV ads.[48]

In summary, OSNs connect consumers and advertisers (two values). In line with value 1 data is collected and aggregated. Based upon this data, business analytics generate value 2. User preferences are inferred from profiles, contacts, clicking behaviour, etc., and used for direct targeting. Associated pricing models enable the three variants: CPC; CPA; and CPO, according to which personal data are marketed.

3.4 LEGAL PERSPECTIVE

From a legal perspective it is not possible to describe online social networks by way of one law which regulates OSNs or establishes some kind of framework for them. Nonetheless, OSNs are not a legal vacuum where everyone can do as they please without consequences. There exist illegal OSN practices which are governed on a national or local level.

The legal evaluation of OSNs is influenced by fundamental rights as well as other regulations. Fundamental rights include the protection of personal data in Art. 8 CFREU (Charter of Fundamental Rights of the European Union), the right to privacy in Art. 8 ECHR (European Convention on Human Rights) and various basic rights provided by the German Constitution ("Grundgesetz"), among them the right to informational self-determination and other personality rights (Art. 2.1, 1.1 GG).[49] But there is a wide variety of other regulations as well. The following chapter will provide an overview of relevant regulations applicable when

48 Future of Advertising 2011.
49 Buchmann 2012, pp. 286-293.

dealing with OSNs, starting with the data protection law as the most significant one, and following with intellectual property, criminal, and copyright law, equality of treatment, and regulations concerning the protection of minors.

3.4.1 DATA PROTECTION LAW

Data Protection Directive

Data protection law in Europe is mainly specified by the Data Protection Directive 95/46/EC (DPD)[50] and the Directive on Privacy and Electronic Communications 2002/58/EC (ECD).[51] However, the Directives generally only bind the national legislator and need to be implemented into national law. The following section will discuss the principles and requirements of the European directives and particularities of German regulations.

When processing personal data of their users, OSNs are considered "controllers" as defined in Art. 2 lit. d) DPD and thus responsible for the lawful processing of that personal information. Thus they must comply with the provisions and regulations of the national laws which are based on the European Directives.

According to the principle of purpose (Art. 6.1 lit. b) DPD) personal data can only be processed for the purpose it was originally collected. The principle of necessity (Art. 6.1 lit. c) and e) DPD) requires the collection, processing, and usage of personal data to be limited to the purpose for which it was collected. Personal data may be processed if the data subject gives her consent, or if it is necessary for the performance of a contract or legal obligation, or for the realisation of another legitimate interest pursued by the controller (Art. 7 DPD).

Data subjects have the right to information whether the data was obtained directly from the data subject or not (Art. 10, 11 DPD). In either case, the data subject has a right of access to the data which includes the confirmation whether or not data has been collected, and the rectification, erasure or blockage of data if it does not comply with the Directive and notification to third parties (Art. 12 DPD).

The above-mentioned principles are implemented into German law, namely into the Federal Data Protection Act (Bundesdatenschutzgesetz, BDSG) and the Telemedia Act (Telemediengesetz, TMG). Two fundamental principles of German data protection law do not have any European equivalent, however. Those are the principle of direct gathering and the principle of data avoidance and minimisation. The first principle requires the personal data to be gathered from the data subject herself (§ 4.2.1 BDSG), so that the data subject is always aware of the personal data that is collected from her. The principle of data avoidance and minimisation (§ 3a.1 BDSG) requires the collection, processing and usage of personal data to be as low as possible. It also addresses technical considerations, because it requires the data processing systems to collect as little personal data as possible.

Categories of data

European legislation does not distinguish between different categories of data. However, the German law distinguishes fundamentally between account and usage data. Each category then follows its own processing rules. Since OSNs are telemedia service providers as laid down in § 2.1 No. 1 TMG the data categories fall under the Telemedia Act (Telemediengesetz – TMG) Following §§ 11 et seqq. TMG, account data (e.g. all registration data such as name or address) may be processed as far as this is necessary for the performance of the contract.[52] Usage data (e.g. user name, IP address, time and volume of use, cookies, identification or transaction numbers) may be processed as far as necessary for allocation or billing of the service.[53]

50 EU Directive 95/46/EC L 281, p. 31-50.
51 EU Directive 2002/58/EC L 201, p. 37-47.
52 Spindler/Schuster 2011.
53 Spindler/Schuster 2011.

All user-generated content cannot be categorized as account or usage data because they are not necessary for the performance of the contract. User-generated content is known is "content data", e.g. posts and comments on personal profiles, status updates, uploaded pictures, or videos. The processing of content data falls under the general rules of §§ 28 et seqq. BDSG. Following § 29 BDSG[54], content data may be processed for the purpose of advertising, in particular if there is no reason to believe that the data subject has a legitimate interest in ruling out the possibility of collection, recording, or alteration (No. 1) or if the data can be acquired from generally accessible sources (No. 2).

Further legal problems

The major problems that arise when dealing with OSNs from a legal perspective are: to what extent EU and the respective national data protection law is applicable to OSN operators, how to better enforce data protection law, and the exclusion of data collection for personal and family purposes from data protection law. They will be addressed in the next sections.

According to Art. 4 DPD and subsequently § 1.5 BDSG German data protection law applies if data is processed within Germany, regardless of the fact that the operator may be registered outside the EU (e.g., the major OSNs Facebook and Google+). However, it is argued under which conditions and circumstances data processing can be considered to have taken place in a specific country – especially when the server storing all data is physically located outside that country. Therefore the scholarly dispute about in which cases German data protection law is applicable for OSNs from outside the EU is still unresolved.[55]

Since OSNs process personal data transnationally, the different national laws make it hard for providers and users to know which data protection regulations need to be observed in which specific context. Even though legal unification progresses in limited dimensions[56], a worldwide data protection law is not in sight. Therefore, other standards of data protection need to be found. Even if EU law is applicable in a certain case, it remains difficult for users to protect and enforce their rights against network operators, especially if the company is situated outside Germany or the EU. The right to delete one's data cannot actually be enforced for most users on OSNs. Even if users were easily able to find out under which jurisdiction their personal data was being processed, when an OSN provider does not comply with their wish for deletion, or if the users want to verify deletion, etc., they will often have to enforce their rights in foreign jurisdictions. Even if some few people are willing to go to such lengths[57] many people would be unable to do so without professional legal counsel.

OSNs are often used by private persons for widely personal reasons. Therefore, vast amounts of personal data are uploaded by OSN users every day. It needs to be discussed who bears the responsibility for the lawful processing of that personal data. This problem arises because according to Art. 3.2 DPD data processing does not fall under data protection law if it is processed mainly for personal or family reasons. In order to establish effective protection of personal data under data protection law, as much data as possible should be defined under the DPD and respective national law. For lack of an explicit legal regulation, it must be carefully evaluated if the data processing is for personal usage or not. One way to prove that usage goes beyond personal or family reasons can be the purpose of processing, e.g. to establish professional or commercial contacts or if the user pursues political or charitable motives (e.g. Facebook's Fanpages).[58] Another clear indication against personal usage is if the data is publicly accessible, e.g. via search engines or if the information is

54 Simitis 2011.
55 Nolte 2011, p. 236, p. 239; Moos 2011; Moos 2012, p. 151; Hoeren 2011; Jotzo 2009, p. 232.
56 Draft for a Data Protection Regulation 2012.
57 See Europe versus Facebook 2012.
58 Jandt/Roßnagel 2011, pp.160 -162.

not restricted to closed OSN groups.[59] For third parties' personal data that is uploaded by a user, both the OSN provider and the user share responsibility for the lawful processing of that data. Basically, the user is responsible for her generated content. If the third party demands protection, e.g. by deleting her data, the provider has to weigh the user's interests in presenting her personality and social environment against the third party's interest in informational self-determination.[60]

3.4.2 EXISTING REGULATIONS INDEPENDENT OF ICT

Apart from the regulations concerning data protection and data processing within social networks there are also regulations which are independent of specific communication technologies but are nonetheless applicable in an OSN context. They will be discussed in the following section. These regulations are intended to protect the individual's honor and dignity or to protect privacy by either reducing possibilities of using public information or distributing it without consent. In some areas of law there is a wide variety of European legislation, whereas other areas are regulated on a solely national level. International and European legislation will be discussed as necessary.

German criminal law provides regulations in §§ 185 et seqq. StGB (Strafgesetzbuch – German Criminal Code)[61] which prohibit defamatory or false statements about a person. That includes statements regarding the individual referred to and statements about third parties. This applies to the OSN context as well, hence defamatory and false statements on one's own or any other profile about a person ("cyber-bullying") are prohibited by law, can be prosecuted, depending on complaint, and will be subject to penalties. Furthermore, illegally impairing someone's personality rights or right to informational self-determination gives the affected person possible claim for injunctive relief against the service provider or the specific user (§§ 1004.1, 823 BGB).[62] Defamatory statements on OSN profiles can impair someone's personality rights, and the right to informational self-determination can be compromised by using someone else's personal data without authorization or permission, e.g. creating a fake profile with someone else's name, picture, or other personal information without their consent.

A lot of personal information about a person can be found online, often because it was made public on an OSN. Information as sensitive as religious or sexual orientation is available, not to mention profile pictures which can give information about gender and race. Depending on the individual privacy settings, that information may even be accessed by third parties. When an applicant applies for a job, the decision-maker (e.g. human resources) might use that kind of information to find out more about the person than is written on the resumé. A range of European Directives address the equal treatment of men and women, including the Employment Equality Framework Directive 2000/78/EC[63] and the Equal Treatment Directives 2006/54/EC[64]. These directives are implemented into the German General Equal Treatment Act (Allgemeines Gleichbehandlungsgesetz, AGG), which prohibits employers from denying candidates (or terminating them) because of certain characteristics or features. These include race, gender, religion, disability, age, and sexual orientation (§ 1 AGG).[65] Hence, an employer is not allowed to use that information to deny a candidate a job position or to terminate the contract. He will be liable for any damages in case of violation

59 Jandt/Roßnagel 2011, pp. 160 -165.
60 Jandt/Roßnagel 2011, pp. 160 -164; Spindler 2012, F 81.
61 There is no European legislation concerning criminal law because the EU does not have legislative power in that area of law.
62 For a detailed overview see Kartal-Aydemir/Krieg 2012, pp. 647-652.
63 EU Directive 00/78/EC.
64 EU Directive 06/54/EC.
65 Other countries have similar anti-discrimination laws, some of them banning the disclosure of personal information in an application.

(§ 15 AGG). So theoretically, even if a user provides information on her profile she should not need to worry that it has negative influence on her work life. Of course, in real life that is hard to imagine and even harder to verify.

The right to personal image is a basic right and protects against secret or forced photography or recordings of any kind, and their distribution. German law provides a protection of personal images in §§ 22 et seqq. Kunsturheberrechtsgesetz (KUG, Copyright Act for Works of Art). To distribute it to the public the person portrayed needs to give her consent (§ 22 KUG). The consent is dispensable in only a very few cases, e.g., with regard to pictures portraying an aspect of contemporary history or when the picture was taken at public events the person attended (§ 23 KUG). On OSNs, pictures of people are uploaded either on one's own profile or another user's profile millions of times, often without regard for the user's consent. The portrayed person has a right to be asked beforehand or to have the picture removed.

Intellectual property law is also applicable to OSNs. The Multimedia Directive 2001/29/EC[66] guarantees and enforces reproduction and distribution rights for creative works of any kind, including computer programs, performances, broadcasts, films, and music (Art. 1-4 Multimedia Directive). The directive is implemented into the German Copyright Act.[67] Within a social network there are two main ways of sharing pieces of work such as texts, photos, videos, or songs.[68] One is uploading a copyright work, the other one is social sharing or embedding content in a user profile. The legal evaluation is not yet consistent. It can be presumed, however, that at least uploading copyrighted works is a breach of the Copyright Act, unless the originator consented, e.g. by implementing a share-function (e.g. "Like"- or "+1"-button) himself.[69]

Regulations concerning the protection of children and adolescents can neither be found in European law acts nor in specific national data protection acts, but rather in the Interstate Treaty on the Protection of Minors (Jugendmedienschutz-Staatsvertrag – JMStV). Its goal is to protect minors and adolescents from content in electronic information and communication medias which impairs or harms their development and education or violates human dignity or other legal goods protected under the German Criminal Code (§ 1 JMStV). Specific data protection laws are not included in the goals of that treaty.[70]

Furthermore, minors are restricted by law when it comes to consenting to a contract. The German Civil Code provides regulations that a minor under the age of 7 cannot consent to a contract at all (§ 104.1 Bürgerliches Gesetzbuch – BGB), and between the ages of 7 and 17 only when the contract has no legal (not economical) disadvantages (§ 107 BGB). The consent to a contract with the OSN provider usually includes accepting their terms and conditions which regularly involve regulations at the expense of the consumer (which would be the minor in this case). That is accepted as a legal disadvantage.[71] Also, the contract would allow the processing of personal data by the OSN provider which has negative effects on the minor's right to informational self-determination.[72] Therefore, a contract with a minor would not be binding without the parent's consent, and the processing of the minor's personal data would be unlawful.

66 EU Directive 01/29/EC.

67 The German Copyright Act guarantees and enforces rights of creative works in literature, science and art (§ 1 UrhG (Urheberrechtsgesetz, Copyright Act)) similar to the Multimedia Directive. The originator of a work has the exclusive right to distribute, reproduce his or her piece of work or make it publicly accessible (§§ 15 et seqq. UrhG).

68 Sievers 2012, p. 229.

69 Sievers 2012, p. 229, p. 231.

70 Jandt/Roßnagel 2011, p. 637, p. 641.

71 Jandt/Roßnagel 2011, p. 637, p. 639.

72 Jandt/Roßnagel 2011, p. 637, p. 639.

3.4.3 CONCLUSION

There is a wide variety of different legal regulations protecting all kinds of legal goods. There is not a single law which is applicable to OSNs, but all kinds of different laws which, put together, provide a fair, though imperfect basis for the legal evaluation of OSNs.

3.5 SUMMARY: AN INTERDISCIPLINARY VIEW OF OSNs

We conclude by summarizing and integrating the viewpoints of the different disciplines in order to provide an interdisciplinary view of OSNs which will serve as a basis for the rest of this document. This summary will stress the most important facts from the viewpoints of the different disciplines.

Firstly and most importantly, users leverage OSNs for social interactions by revealing and concealing themselves in an interplay with other selves. Paradoxically, OSNs bring this interplay to a broader, digital stage while at the same time limiting the closeness of the encounter. OSNs are mainly used to maintain social relationships generated in the offline-world and hence they are increasingly organised around people rather than interests. For some user groups (e.g. youth), using OSNs is mandatory to keep up with their social networks; thus OSNs assist in generating sociality in a very serious sense. The integration of a broad range of communication tools and multimedia applications make OSNs even more attractive for users, mostly because they provide means to share information as well digital data items; as sharing is to be understood as a key mechanism for generating and maintaining sociality the features that make sharing possible help to strengthen social bonds via OSNs. Hence, the usage of OSNs boils down to sharing information between self-determining selves; and all this information is mediated through OSN operators which in turn usually offer the corresponding services for free. To be able to offer these services for free while at the same time generating some revenue, OSN operators market the information provided by users. To this end, OSN operators do not only act as intermediary between OSN users, but also as an intermediary between customers (which usually correspond to OSN users) and advertisers (usually companies). By means of smart data collection and data usage (e.g. data inferences), advertising in OSNs is more effective than traditional types of marketing. Another aspect of OSNs is that they are telemedia services and thus their providers need to comply with the German data protection specifications in §§ 11 ff. TMG and the BDSG if they are seated in Germany or if they are seated outside the EU but process personal data in Germany. Because of the internationality of OSNs it is especially challenging to enforce data protection regulations with OSNs. Also, it is not easy for users to find out under which jurisdiction their personal information is being processed.

3.6 THE BENEFITS OF ONLINE SOCIAL NETWORKS

In this chapter, we discuss how online social networks (as characterized in Chapter 3) might contribute to realizing the core values (as defined in Chapter 2). We outline characteristics which should be retained and fostered when proposing options for modifying sociotechnical practices of OSN usage. We begin by specifying OSNs' capacity to help actors in accomplishing self-determination (4.1). Subsequently, we illustrate OSNs' potential to foster democratic participation (4.2), followed by a discussion of how economic well-being stands to benefit from OSN features (4.3). In the concluding section, we will present a short summary (4.4).

Before elaborating on these issues, we add one more "technical" remark. Throughout the chapter we draw from our own research[73] as well as from relevant research literature. The latter includes quantitative as well as qualitative research. The more abstract and general assertions we present are derived from the body of literature referring to research on

[73] Buchmann 2012.

OSNs conducted in Western environments (Germany and the US). We also draw on an anthropological study of Facebook usage accomplished in a non-Western setting, namely in Trinidad. Trinidad is a Caribbean island located a couple of kilometres off the Venezuelan shore. The reasons for taking this research into account are threefold: first, in this literature we find in-depth ("thick") ethnographic descriptions of the actual practices that people develop on OSNs; those descriptions allow us to illustrate some of the more abstract arguments that we put forward. Secondly, the fact that those examples come from research within a non-Western setting allows us to conclude that the potential benefits of OSNs specified by us are cross-culturally valid and therefore genuinely linked with the horizon of possible uses of OSNs - not only to a specific sociocultural setting (such as "the West", e.g. Germany). Thirdly, as we deal with the *potential* of OSNs in this section, turning the lens to a non-Western setting might make potential benefits visible that are not realized by users in a German or US context, but that are nevertheless worth preserving. We would ultimately like to stress that the case of Trinidad only serves as a proxy here. The study we draw upon is simply the best and most up-to-date anthropological research on OSN usage in a non-Western setting that we could access. It is well-suited for enriching our account of OSN's capacities for realizing the core values as they were specified in Chapter 2.

3.6.1 THE BENEFITS OF OSNs FOR FREE SELF-DETERMINATION

Opportunities for interaction

While in several respects interaction – the interplay of the self with other selves – lays the foundation for free self-determination, OSNs multiply the opportunities for such interactions. The average number of "virtual friendships" on Facebook, for example, is 130[74]. Of course, these "friendships" are not to be understood in the conventional sense of the word as other selves with whom an actor has a close relationship; rather, they are potential *interaction channels* that can be actualised easily, and that allow for interacting with an extended circle of acquaintances. In particular, these channels might lower the threshold for communication considerably, as they remove physical boundaries, extend the scope of communications geographically in an almost unlimited way, and heighten the probability of communicating with people with whom one has only the weakest of ties. There is no need to address someone directly, as the audience to be addressed is composed of several recipients and therefore rather diffuse. In this sense, posting a message can be easier than sending an email. Last but not least, there is a range of different channels (private mail, post, chat), allowing the user to choose the actual mode of communication (synchronous, asynchronous, one-to-one, one-to-many). Thus, OSNs multiply the opportunities for interplay with other selves in a quantitative way.

Identity formation

OSNs also modify the quality of the modes of self-determination. Whereas the interplay with other selves enables an actor to develop his or her (multiple) identities, there is a manifold of existential options originating from the OSN world, which can be integrated into the process of building one's self. It is important to note that these options are different from those existing in the offline-world.[75] For example, on OSNs an actor has a manifold of features at his/her disposal for expressing likes and dislikes, and for self-definition by sharing a range of media, such as pictures,

74 Wang et al. 2011.

75 While Benkel notes that there are really novel ways of constructing one's personality, his essay on "visualization strategies" on Facebook is characterized by a remarkable ambivalence concerning the status of OSN social processes. He notes that visualization of Facebook is not about showing one's empirical personal character ("wie man ist"), but about presenting someone the user would like to be ("wie man sein kann und will"). Referring to self-determination as a constant, never-ending process of creating a self, from our point of view Benkel's distinction is misleading. OSNs provide for novel ways of creating a self, it is however, unfruitful to specify OSNs features against the background of some illusory, pure and unmediated human social reality, for the social is generally impure, mediated, in short: *socio-technical*. Benkel 2012.

movies, music and so on. As boyd has shown, young users draw most frequently on these resources for defining their personality.[76]

Social inclusion

With OSNs comes an increased pool of resources that contain features which are attractive for actors who dwell at the edge of the social periphery. Anthropologist Daniel Miller reports how a shy and rather marginalized Trinidadian makes use of Facebook's online game "Farmville" for establishing a self in relation to his group of colleagues.[77] Playing the game incites communication between the player and his colleagues in the offline world as well, for via the game the players share a common interest. In this way, OSNs have the potential to include the excluded. This aspect relates to the opportunities for self-expression created by OSNs, and thus for sharing one's worldview, for expressing political, religious, sexual preferences, and so on. An actor might share his or her convictions with like-minded actors, gaining support, thus strengthening one's worldview.

Impression management

Another integral element of self-determination is the technique of "impression management." The latter concept was developed by Erving Goffman[78] and refers to the everyday activity of drawing a picture of one's self *vis-à-vis* the social network one is, or would like to be, part of. Playing a role in the social network pre-supposes learning how to play while learning to play a role is in turn tied to learning what information to give away and what information to hide – the play of concealment and disclosure. Actors can use OSNs for impression management. Given that concealment/disclosure is one of the key social skills needed to develop one's personality, OSNs serve as a playground, a social space for learning this kind of skill. On OSNs it is easier to wear and test various selves, for the masks one might possibly wear are less defined by physical, e.g., bodily or psychological restrictions.

Overcoming real-life boundaries

In this context, we may once again refer to the anthropological example of a shy guy playing "Farmville" that was cited above; another case Miller presents is a sociable former human rights attorney who, due to a disease and the handicaps that come with it, has few chances to socialize in the offline world. However, via Facebook he maintains existing relationships and even creates new ones with people living abroad.[79] The example demonstrates that there is a certain freedom within OSNs from some of the offline world restrictions. In this respect, boyd too, when presenting ethnographic research accomplished in a US context, highlights the fact that the opportunities for youth in everyday life to indulge in the task of self-determination are severely restricted by all kinds of authorities (she mentions parents, teachers, and government officials;[80] we might add colleagues, bosses, police etc.). OSNs provide a space that, to a certain degree, can be free from the confines established by those authorities.

Entrepreneurial opportunities

The last thing we would like to account for in respect to the core value of self-determination turns the lens from the users to the providers of OSNs. Quite a few of the early OSNs owe their existence to more or less visionary ideas developed by Web 2.0 entrepreneurs. Establishing an OSN platform requires technical skills as well as the capacity to translate the technical network into a sustainable business model. In Germany, Art. 12.1 GG grants actors the right to choose a profession and establish an enterprise. Thus, if being an OSN entrepreneur is part of one's self-definition, the opportunity to establish an OSN and gain money from it is firmly tied to the core value of self-determination. For this

76 boyd 2007.
77 Miller 2012.
78 Goffman 1973.
79 Miller 2012, pp. 88–103.
80 boyd 2007, p. 19.

reason, the socio-technical, socio-legal, and socio-economic environments should preserve opportunities for entrepreneurs to create and maintain OSNs.

3.6.2 THE BENEFITS OF OSNs FOR DEMOCRATIC PARTICIPATION

Establishment of networked publics

As was stated in chapter 2, public self-expression and the opportunity to participate in social occurrences is a precondition for democratic participation. As OSNs can be used to participate in social networks, that is, to partake and also benefit from those networks, they have the capacity to contribute to democratic participation.

OSNs might be understood as "networked publics", or as "one type of *mediated public*. The network mediates the interactions between members of the public."[81] Establishing audiences and sub-audiences in OSNs creates networked publics. While having one's say and paying attention to what somebody says in these publics fosters democratic participation, the networked publics of OSNs are different from those of the physical world insofar as OSN publics are characterized by *persistence* (the information fed into an OSN does not disappear after it is expressed), *replicability* (one can copy information as many times as one likes), *invisible audiences* (the audience is invisible insofar as it is not necessarily present at the event, i.e. because of the persistence of the information, there may be a future audience, unknown at present, to be taken into account) and *searchability* (it is detectable using search engines).[82]

Audience selection

At first glance, the number of ways to choose one's audience is significantly increased in OSN publics. As it becomes possible to easily address numerous actors, using OSNs augments participation considerably. OSNs overcome some of the limits of physical public space. In this sense, in "unmediated environments, the boundaries and audiences of a given public are structurally defined";[83] in OSNs, however, it is generally possible to shape the structure of the public to be addressed by dividing one's network into sub-groups. In principle, this also increases the individual's capacity to be freed from structural limitations and overly restrictive social rules, that is, to communicate without being observed by social authorities of various kinds (here, again, referring to parents, teachers, colleagues, employers, policemen etc.[84]). The perfection of OSNs then, is that the public aspect of OSNs is both free from physical and social structural limitations, and adds granularity to the individual choice of the audience to be addressed when expressing one's view. Hence, OSNs can be means for fostering democratic participation.

Accumulation of social capital

OSNs have the potential to foster democratic participation in yet another way. In one sense, democratic participation is about partaking and benefiting from social networks (or from "society", in more traditional language). This is why we must note OSNs' capacity to generate bonding, bridging, and maintained social capital (see Chapter 3). Social scientific research has shown quite plainly that using OSNs, especially by supporting the building and management of weak ties, increases subjective (or psychological) well-being (Ellison/Steinfeld/Lampe 2007)[85]. In this sense, OSN users do indeed benefit individually from interactions and memberships in OSNs. Thus, as OSNs bring about opportunities to take part in and also to benefit from social formations, we can state that they foster democratic participation. Of course, the term "democratic" might be understood in a more strict sense, thus introducing further conditions to be fulfilled by OSN interactions in order to be consistently defined as

81 boyd 2007, p. 8.
82 boyd 2007, pp. 8-9.
83 boyd 2007, p. 8.
84 boyd 2007, p 18.
85 Ellison et al. 2007, pp. 1143–1168.

fostering "democratic participation." As we have seen above, in a broad sense "democratic" refers to actors' opportunities to negotiate and have knowledge of the rules of the social game to be played. In fact, on OSNs actors can learn to apply these rules as well as partake in their negotiation: Online social networks constitute social arenas for developing skills in establishing, applying and negotiating norms that are valid in their peer group.[86] Moreover, as was noted in chapter 3, influential classic social theory holds that gift economies serve the function of establishing social relationships (Mauss 1968)[87]. Sticking to this presumption, we may understand the multiple options to share content in OSNs (videos, music, and pictures) as a formidable way for establishing and strengthening social bonds. For example, Miller reports how the Trinidadian attorney mentioned above decisively deepens his relationships to London-based expats by exchanging classic Trinidadian music MP3s and the like.[88] So, having various options for sharing allows members to partake and to benefit from social networks; in this sense, providing features for sharing content is yet another way OSNs may contribute to democratic participation.

Formation and expression of political will

While democratic participation is about politics, the latter might also be understood in the more narrow sense of forming the explicit political will of the polity: the sovereignty of the people culminating in the opportunity of each citizen to freely choose his or her representatives (in representative democracies) during the course of elections, especially parliamentary elections.[89] Participation in elections is, of course, not directly influenced by political information revealed in OSNs. Users might reveal whom they are planning to vote for or whom they have voted for in the past. Still, since election content is kept secret, nobody will be able to determine the validity of such a statement. Thus, even if users are discredited for the revealed election behaviour, this will not likely coerce them into making specific decisions when voting in future elections.[90]

As was established above, free choice and free decision making in elections presupposes, that each citizen has the right to form an opinion on an issue. Therefore, another very important sphere of democratic participation, which subsequently culminates in elections,[91] is the free public formation of opinion.[92] The right to partake or not in this social exchange actively or passively is protected by the Freedom of Opinion and the Freedom of Information clauses in Art. 5.1 GG and the Freedom of Demonstration clause in Art. 8.1 GG. Indeed, to form an opinion, citizens must have the means to gain information and to exchange opinions in political discourse. Freedom to express political opinion and to gain information, which are viewed as highly important for the democratic process,[93] are supported by OSNs, for OSNs have a manifold of features on offer that allow for political discourse to flourish. As OSNs help to establish publics, they support public discourse and enable each citizen to learn about the variety of opinions concerning an issue. More specifically, they make it possible for anybody to have one's say as well as to pay attention to what somebody says. In this sense, OSNs have the potential to guarantee freedom of speech and to stage dispute and contestation through public discourse. Citizens gain the opportunity to express political views and party affiliations and to influence numerous people. It is thus possible to be informed about other people's political views and affiliations to parties or enterprises and consequently easier to evaluate, if one in fact wants to follow a particular person's political

86 boyd 2007, p. 21.
87 Mauss 1968.
88 Miller 2012, pp. 98-99.
89 Meyer 2005.
90 Schreiber 2009.
91 Dreier 2006.
92 Kloepfer 2005.
93 Jarass 2007.

lead or even vote for that person in an election. The bottom line is that the opportunities for expressing one's opinion and gaining information improve. In this way, democratic participation is improved as well, since the decision process is enriched with relevant information.

The recent past has shown that it is not only some representative space, such as the parliament, or some distinguished public sphere where political issues are articulated. In the case of the controversy surrounding the re-construction of Stuttgart's main station (*Stuttgart 21*)[94], the extension of Frankfurt's Rhein-Main Airport[95], and the upheaval in several Arabian countries (termed "Arabellion")[96], OSNs have demonstrated their potential to serve the purpose of self-organizing people around issues, that is, of organizing rallies, protests and even supporting regime change from a grassroots level. Rallies and demonstrations can be understood as public process of opinion formation. The right to demonstrate without interference by governmental or other authorities in public areas is laid down in Art. 8.1 GG. Granting this right is viewed as especially important for the democratic process.[97] As OSNs can be quite effective avenues for organizing such events, including the flow of people and information required for this kind of self-organisation, the integrating effect of demonstrations can be improved by OSNs.

3.6.3 THE BENEFITS OF OSNs FOR ECONOMIC WELL-BEING

Employment and generation of profits and tax revenue

Triggered by increased connectivity and reduction of search and distribution costs, the Internet economy changes the terms of trade. As consequence and extension of e-commerce, OSNs involve all stakeholders in the process of value creation. While e-commerce offers products in a client-server scenario, the key success factor of OSNs is cooperation with regard to economic impact. According to a recent study, Facebook contributes significantly to economic welfare in Europe. An economic impact of €15.3 billion and the support of 232,000 jobs across 27 European countries and Switzerland were estimated for the year 2011.[98] Welfare distribution is possible from increased employment wages, taxes paid, and profits generated by both Facebook itself (direct effects) and the companies using Facebook (indirect and induced effects). Direct effects are owed to the fact that OSNs are business models themselves. They generate profits, pay taxes, and employ people. Indirect effects come about when clients of OSNs use the service infrastructure for the more efficient promotion of their own products and services. Some of them contribute to the growth of app communities, e.g. providers of online games and other economically relevant applications. In this role OSNs are platform providers for supply-chain industries. The indirect effects of OSNs originate from third parties building their business models on the most adequate OSN platform. Induced effects reinforce direct and indirect effects of OSNs and their suppliers, e.g. the more companies participate on the platform the more attractive is the OSN and its third-party applications (network effects). For some businesses, OSNs also provide an infrastructure to offer their own services, e.g. shopping apps. Indirect effects within the induced effects stimulate sales of infrastructure providers and hardware suppliers, e.g., smartphones and broadband connections. In addition to the benefits gained by individual users, companies generate new sales by advertising their products and services through the social network. OSNs provide

94 In the case of Stuttgart 21, both supporters as well as adversaries created Facebook accounts in order to gain support. (FÜR Stuttgart 21 2012); (KEIN Stuttgart 21 2012).

95 For example, there is a blog of Northern Frankfurt residents who are adversaries of the Rhein-Main Airport extensions (Fluglärm Mainz 2012) while residents of Mainz have opted for a Facebook account (Frankfurt Nord 2012).

96 While there is controversy concerning the weight of OSNs and other social media, there is only little doubt that these technologies did play some role in the Arabian upheavals. For a perspective highlighting their role see Hirschkind 2011. A more cautious view is presented in Deutschland Funk 2011.

97 Jarras 2007.

98 Deloitte 2012.

platforms to promote and advertise products, services and to increase brand awareness. In an economic transaction they are intermediaries.

As intermediaries, OSNs decrease the cost of performing economic transactions. Cost reductions are related to three effects that have been studied in the context of e-commerce.[99] For e-commerce - and even more for OSNs - specialization enforces the concentration on core competencies. Specialization is a characteristic of any economic development since the advent of the industrial revolution, and is even more crucial for e-commerce. Secondly, specialization increases costs of coordination. However, as intermediaries between market participants, OSNs reduce coordination costs. Thirdly, cost reduction in coordination requires sophisticated cooperation technologies. In recent times, "wisdom of the crowds" has become a major driver for the reduction of transaction costs. O'Reilly's seven principles describe the intelligent Web, based upon cooperation through collective intelligence.[100]

3.6.4 SUMMARY: THE BENEFITS OF ONLINE SOCIAL NETWORKS

We conclude that there are various benefits OSNs have to offer when it comes to strengthening the core values. In some cases, the benefits brought about by OSNs' features concern even more than one core value. For example, while OSNs' networked publics can be organised around people or around issues,[101] organizing people around issues may create close relationships,[102] thus simultaneously supporting self-determination and democratic participation. Similarly, creating an environment that allows entrepreneurs to establish an OSN business might contribute to economic well-being as well as to self-determination. For a variety of reasons, then, the features safeguarding the benefits of OSNs are worth being maintained and fostered. Simultaneously, some of these features may have considerable drawbacks, which will be explored in Chapter 5.

99 Müller et al. 2003, p. 302-304.
100 O'Reilly 2005.
101 For example, networked publics can be organised around a common political goal, that all the public's participants pursue (resistance against the Rhein-Main Airport's extension or the like); or they can be organised around people themselves, as in the case of managing peer groups via OSNs. See also boyd et al. 2007.
102 Miller 2012, pp. 88-103.

4 CHARACTERIZATION OF E-COMMERCE

4.1 E-COMMERCE FROM AN ECONOMIC AND TECHNICAL PERSPECTIVE

Electronic commerce (e-commerce) is identical to traditional commerce, except the market is virtual and operated by technical information systems, i.e. e-commerce is also called virtual market. In these markets, sellers and buyers meet under pre-specified conditions. These conditions are the topic of an innovative economic research area called "market design", and this defines and limits the flexibility of the relative position of market participants most often by using price as a parameter.Since e-commerce accounts for almost 30% of German trade, trust in the infrastructure and in the relationship of sellers to buyers will decide the future contribution of e-commerce to economic well-being of an advanced society.E-commerce here is used in an inclusive sense, handling the push of technology as well as the market pull to actually generate and maintain electronic markets.

Due to information technology (IT), electronic markets need to be designed and pre-specified with an engineering mindset. Market design has to take into account both the supply side as well as the demand side. While suppliers prefer a free unregulated market, consumers desire protection. Thus technology and market characteristics may influence the supplier-consumer relationship with regard to awareness, control and trustworthiness, especially on the consumers' side. These information systems represent an Internet-based sales channel enabling buyers to find sellers matching their needs. E-commerce usually refers to all kinds of commercial transactions and business processes (e.g. online advertisement, online banking, etc.)[103]. E-commerce has experienced rapid growth in the last 16 years. This evolution is an agreement amongst the participants, who freely select their most convenient and profitable forms of economic interaction in a market. E-commerce has experienced distinct technical stages where the transition from one stage to the other can be traced back to a struggle between buyer and seller.

Advanced technology leads to reduced search costs for the buyers, while sellers use technology to retain these buyers by increasing their switching costs. Switching costs emerge for the customer when changing their preferred provider. The costs can occur in several forms, for example, creating a new account, getting acquainted with another online shop, reading terms and conditions, losing access to additional services like social shopping and useful recommendations or by losing convenience coming from stored personal data. Trust in one seller also creates switching costs, if the level of trust in other sellers is lower. The amount of switching costs depends primarily on the design of markets and secondarily on technology. If, for example, the portability and transparency of user data and profiles would be a characteristic of a given electronic market, this could reduce switching costs for all sellers and may take away a competitive element. A reduction of search costs is in the interest of buyers when they try to obtain information about prices and products.[104] At the same time search cost reduction reduces profits of some sellers, if the buyer has an option to switch. In consequence sellers aim for higher switching costs. Within the present stage of technical development of e-commerce – which may be called cooperative e-commerce – the seller collects personal data to provide the best supply for the demand and to bind the customer with services beyond the narrow scope of his purchase. Knowing the customer is a means to increase switching costs. In the history of e-commerce, technology has been in favour of buyers since in the majority of cases search costs were reduced[105] and markets became more transparent by advances of technology. This contributed to an uncertainty of sellers. Sellers were forced to invest in technology to upkeep switching costs and to maintain a stable customer base. Here however, two cases must be distinguished. In a market where

[103] Müller et al. 2003.
[104] Laudon/Traver 2007.
[105] Brynjolfsson 2009.

commodity products are traded, improved technology leads to increased market transparency, thus increasing control of buyers. In more sophisticated markets, however, with heterogeneous product offerings and advanced consumer tastes, sellers are forced to improve awareness of their specific offerings to increase control and trustworthiness[106]. This challenge to adapt to technical progress with uncertain return of investments has increased the desire to "know the customer" much better, and has required collecting personal data to adapt to market changes. The collection of personal data has the objective of learning what buyers need and to match market supply to the demand of customers at lower cost[107]. Thus e-commerce, in its forthcoming developmental stage, may be characterized as data-centric.

4.1.1 E-COMMERCE STAKEHOLDERS

E-commerce has the same stakeholders as does any well-known traditional commerce with the exception of the suppliers of technology and the operators of electronic markets. They are known as "support services", and generally include all types of Web 2.0 services. The economic Nobel Prize laureate A. Roth has studied relationships of E-markets in order to specify rules for markets, and at the same time to continue to allow free establishment of prices based upon supply and demand.[108]

Customers

Contrary to regular markets, preferences of customers can be collected at any transaction or even from basic interaction with the e-commerce platform. Customers' desired convenience level, price threshold, and the degree of choice available are the three properties affecting customer behaviour. In Germany, the number of online shoppers increased from 25 Million in 2005 to 34.1 Million in 2010[109]. Customers usually begin a search for products by using a "regular" search engine (58%), followed by visits to sellers' websites (24%) and, more recently, by using social media to either identify a common entrance point for online sales (18%) or contribute directly to product design. This makes the support services an ideal intermediary between customers and sellers, where the customer usually gets free services and supplies personal data to the support service. This may cause an information deficit for the supplier.

Businesses

From the late 1990s to the present, the dominant strategy is to increase market share, which takes priority over profit. In 2008, Amazon announced its first profit. To improve customer relations, the following three factors have been used either alone or in combination: (1) increased technical functionality, (2) increased complexity of product offerings, and, (3) market properties such as size and variety. Amazon is an example of the mixed strategy, applying all three of the above factors to define the relationship with their potential customers. Amazon offers far more than books, and has extended their portfolio to include all items within a stationary, specialized department store. The idea is to improve knowledge about buyers' behaviour in several product domains and thus decrease search costs beyond a single product. The increased complexity is possible due to increased market size and cross domain personal data. By introducing the e-book reader Kindle, Amazon increased switching costs on customers' side in the growing e-book market, while due to Amazon's size and data pool has the means to reach beyond Kindle customers to sell additional offered products. Online auction services like Ebay focus on functional extensions to improve customer-to-customer relations. Social commerce companies like spreadshirt focus on customer to business to directly involve the customer in the value chain by giving them the opportunity to customize products and help to shape the market properties according to individual wishes. In Germany, the ignorance of the

106 Lin 2008, pp. 60-65.
107 Schafer et al. 2001, pp. 115-153.
108 Roth 2008, pp. 285-310.
109 Statista GmbH 2012.

relationship of these three factors to influence search as well as switching costs led to market exits, e.g. by Quelle, while Otto-Versand prospered. From 2005 to 2011, e-commerce turnovers in Germany increased by 80% up to €26.1 billion. In opposition to this development, offline retail turnovers decreased by 0.8% down to €395.9 billion. Businesses are relying more heavily upon support services to maintain a steady level of switching costs.

Administration

In general, public organisations offer services under the name "e-government". The objective is to increase the service rate at lower cost. The technical bases to achieve the goals of businesses and administrations are identical. Public organisations, however, often cannot give customers a choice of how to perform regulated procedures, but they are under more pressure to maintain a high level of awareness, transparency and trustworthiness. One example of Customer – to – Administration (C2A) e-commerce is ELSTER which allows German tax payers to submit applications for online tax return. The new electronic ID card (Elektronischer Personalausweis nPA) enables users to get access to several e-government services, e.g. digital signature services[110].

Support services

Growing complexity of many e-markets, the global reach of e-commerce, and the distribution of value chains of suppliers have caused an information overflow. Information overflow increases simultaneously with search costs and switching costs. Support services are a prerequisite to aid buyers in handling information overflow. Today, the business model of specialised support services acting as intermediaries between buyers and sellers is called "cooperative" and lays the groundwork for future, even more advanced data centric e-commerce.

E-commerce is the operational part of e-markets depending upon classifications reflecting the legal, social and ethical rules understood and accepted by buyers, but it is not limited to exactly one object to be traded. Support services of the intended transaction influence search as well as switching costs. For example, most airline services offer travel insurance, car rentals, and hotel packages in addition to plane tickets. E-market design and the acceptance of its rules depend upon cultural settings. Support services are relatively free with regard to the methods they use for classification. The way in which inferences are generated is not usually transparent.

4.1.2 E-COMMERCE: CO-EVOLUTION OF TECHNOLOGY AND MARKETS

Since its modest beginnings around 15 years ago, e-commerce has undergone a dramatic increase in the number of technical and economic changes. Organisations which operate information systems for electronic trade have turned out to be both intermediaries as well as sellers. For instance, Amazon provides a technical and administrative infrastructure and adopts a role as an independent third party to offer support services. Google and Facebook act as intermediaries only, without taking the role of a seller. Generally, any e-commerce company can act as an intermediary, a market participant, an independent third party, or a consortium of firms or buyers. Usually, e-commerce actors require substantial investments in systems development, but, once in place, they handle larger volumes of market transactions at lower cost than any other form of market organisation. Buyers' decisions to choose one seller over another depend not only on the actual product bought, but also on additional services. Examples are social shopping platforms, tools that ensure convenient shopping like one-click ordering, recommendation systems, and customized products and services that are of interest to buyers though not necessarily product-related. Electronic devices and the usage of specific services in the e-market have become a positive social indication

[110] Scheer et al. 2003.

of the lifestyle of important populations of consumers, which, in addition, has forced sellers to become forerunners in both technology and product ideas[111].

Firms in e-markets face substantial technical and organizational costs if buyers decide to switch to an alternative seller or if their innovation is not embraced. In this case all investments are lost. This investment is not only technology-dependent, but is also influenced by regulations, ethical and social standards, and by law. It has been proven that the forerunner in applying technical progress has usually been rewarded, but often faces problems when they must adapt to regulations not common in the local market of the seller. Often it is assumed that investments in hardware and software, user training, behavioural changes as well as reduction of non-technical barriers, e.g. investments in trust and privacy, are the elements required to retain customers. The fact is that the higher the switching costs are, the fiercer is competition for the uncommitted buyers[112] and the more the customers decide upon product specifications. Examples for such product specifications may include privacy, fair trade, or environmental friendliness in addition to quality and price. The result is to build complex new markets around already existing e-markets considered reputable and trustworthy by their customer base[113]. In complex markets trust and privacy are in high demand, whereas markets for commodity products tend to ignore violations of trust and privacy[114]. Accordingly, ensuring customers' privacy is an important product specification for advanced products which usually goes hand in hand with higher prices[115], since investment in awareness, control and trustworthiness sometimes exceeds the operational cost of the platform offered. Beyond the capability to raise capital and participate in the technical race, it can also be shown that a "good" migration strategy from old to new technologies influences the progress of a specific business. Businesses must offer older services along with new services to keep the old customer base while attracting new customers at the same time[116]. The majority of e-commerce sellers during the Internet hype in the late 1990s were not able to keep pace with technical standards. This led to a loss of customers due to the impossibility of participating in economies of scale. Competitors who could not maintain this speed of innovation vanished from the market. Today, e-commerce shows a trend toward (temporary) monopolies[117], as many of the support service operators are arguably a natural monopoly without the negative impact of monopolies and market performance. If this argument is not convincing, support services may be considered part of a national infrastructure. Regardless, e-commerce reveals the following benefits compared to classical commerce:

- E-commerce reduces customers' search costs for prices and products faster than any other form of market.
- The benefits for sellers and buyers increase the larger and more complex the electronic market becomes.
- The development of e-markets requires high expenditure for establishment and maintenance. These costs are composed of functional expenses, but also of characteristics of market design, especially with regard to trustworthiness.
- The superiority of market-oriented coordination mechanisms over hierarchical management is the source for socio-technical, business, and social innovations.

So far the close relationship of technology and economic rules expressed by the struggle of search costs and switching costs led to a unique co-evolution, which triggered and

111 Mellahi/Johnson 2000, pp. 445-452.
112 Farrell/Klemperer 2007, pp. 1967-2072.
113 Böhme et al. 2007.
114 Kaiser/Reichenbach 2002, pp. 25-30.
115 Müller et al. 2012.
116 Sackmann/Strüker 2005.
117 Müller et al. 2012.

is characterized by a "market pull" and "technology push". Markets of the first phase of e-commerce were designed as a mirror of classical commerce. This form of e-commerce lasted from 1995 till about 2005. It simply imitated the relationship of clients with a physical shop, but it reduced cost and extended product selection. In the second phase, cooperative services involved the buyers in e-commerce by requesting that they share their experiences and opinions about products and services, e.g. via online social networks. Wisdom of the crowds as a factor for progress emerged from user involvement and led to a large collection of data about buyers' behaviours. For instance, crowd sourcing has made Wikipedia superior in speed of updates and quality of information reliability compared to printed encyclopaedias. Customer interaction generated a metric to judge cost versus benefit of each transaction phase in regards to economic value. This knowledge triggered new business models, but also required advanced technology. This transformation to cooperative e-commerce began with the appearance and acceptance of Facebook and other Web 2.0 applications including search engines and recommender systems in 2006. Enabling customers to customize or design products melded the roles of market participants and the concept of a prosumer appeared.

Technology has usually favoured buyers by lowering search costs thereby reducing sellers' profits[118]. With increased complexity the vast amount of information and data available became counterproductive to e-commerce growth and called for another technical push. The result is the appearance of support services. The most obvious change in markets is the entrance of third parties. The other is the deconstruction of the value chain into its individual phases by direct user involvement. The most likely but unintended result is the build-up of "Big Data"[119]. It is claimed that "Big Data" and its analysis will help to predict buyers' behaviour, and holds the potential to influence buyers' behaviour with regard to their perception of search and switching costs[120], which may change the terms and conditions of today's e-commerce market participants.

Today's reality is the fast growth of support services developing methods to classify the information and to collect personal data in exchange for free services to handle information overflow. Decontextualization, persistence, and re-identification become threats to a trust infrastructure, beyond the scope of existing regulation.

4.1.3 CLASSICAL E-COMMERCE: MARKET AND TECHNICAL TRANSACTION SUPPORT

Client-server interaction is the technical term for the first phase of e-commerce. The enduring contribution made by classical e-commerce is the structuring of e-markets according to transaction phases. Transactions are the means to model interactions among users, and technology is the method which supports both buyers and sellers. In classical e-commerce a transaction represented value generation was owned by a single supplier and characterised by the interaction with the buyer. If the buyer was aware of the reputation of the seller the balance of market influence was maintained. As a result, the concept of data minimisation was conceived to guide the aforementioned interrelationship and ultimately became an instrument to ensure privacy.

E-commerce transactions of today are the result of past experiences, common practices, and the adaption of the concept of a transaction as the smallest unit of e-commerce[121]. Transactions can be divided into five phases. The first three phases consist of (1) establishing a relationship (2) bargaining the

118 Bakos 1997, pp. 1676-1692.
119 Buchmann 2012.
120 McAfee/Brynjolfsson 2008.
121 Müller et al. 2003.

terms of exchange (3) performing the exchange of the product of interest. Phases 4 and 5 deal with control and conflict resolution after delivery has taken place and one or more parties claim a violation of obligations.

1. Initiation phase: The goal is to increase buyers' awareness and to establish trust. Sellers try to attract customers by applying the most appropriate technology to reduce search costs. Users often start their search with conventional search engines or with search engines and catalogues of particular shopping platforms.

2. Negotiation phase: In today's B2C and C2C e-commerce, terms such as price, quality, and delivery time of products are subject to negotiation. Signalling the policies of negotiation, and allowing the buyer to screen contributes to a sustainable trust infrastructure.

3. Delivery phase: Delivery includes fulfilment of obligations. Numerous technical web-based solutions have been developed to distribute digital goods to end users: applications, music, games, and movies are distributed via platforms such as Google Play Store, Apple iTunes, Valve's Steam and Amazon Instant Video.

4. Control phase: The German word "Kontrolle" is different from the broader meaning of "control" in English. The semantics of the term "control" also connotes audit, surveillance, and conformance checking once delivery is accomplished. The most popular control technology is a public-key infrastructure (PKI). A PKI is a set of hardware, software, people, policies, and procedures needed to create, manage, distribute, use, store, and revoke digital certificates.

5. Conflict Resolution phase: Traditionally, resolution is done by self-organisation or legal institutions. Unfortunately, the territorial principle of legal institutions, as well as the extensive time required, demanded other technology and organization be created. At present 36% of all complaints are solved by an intermediary specializing in Alternative Conflict Resolution (ACR). One of the most successful companies is Better Business Bureau[122] where more than 1 million complaints are resolved without legal intervention. With regard to security and privacy, ACR has had an influence on US business practices. Ten years ago, in the case of www.toysmart.com, the US Federal Trade commission decided that seals and profiles must remain protected in case of a conflict[123].

4.1.4 COOPERATIVE E-COMMERCE: TECHNOLOGY TO COORDINATE MARKETS

Cooperative e-commerce involves customers in value generation and receives its justification from segmented transactions and information overflow as well as the involvement of crowds. As shown in Figure 1, the service to coordinate both customer interactions as well as the composition of distributed transactions has been taken over by third parties called support services. These are not only OSNs, but all the services described by the popular term "Service-Oriented Computing".[124] Collaborative web applications began to integrate additional services into their offerings to retain buyers and to increase their switching costs. This was accomplished by considering buyers' demand and preferences beyond the purchase of the desired product, e.g. payment services add functionality to online shops beyond product acquisition. Web platforms emerged and allowed consumers to actively participate in the generation of content. The result and consequence of increased buyers' involvement is the generation and collection of user data.

122 Better Business Bureau 2013.
123 FTC v. Toysmart.com, LLC 2000.
124 Kontogiannis et al. 2008.

4.1.5 DATA CENTRIC E-COMMERCE: TECHNOLOGY FOR DATA

The exploitation of Big Data will be the dominant characteristic of the upcoming evolutionary step in e-commerce. Mostly, Big Data is considered a result of the present cooperative e-commerce and a threat to privacy on the buyer's side, and as a source for new business models on the seller's side. This difference of perception is due to increased productivity of sellers[125]. Apple has become the most valuable IT company, since in addition to the popularity of its products, the data available regarding customers' behaviour dominates location-based business and services. It is a justifiable assumption that availability of data increases switching costs and retains customers[126], which may have negative effects on the productivity levels[127], if they become too high. For instance, in physical book stores sellers know what customers bought and what they did not. Once bookselling had moved online and the use of mobile devices had turned into common practice, store managers knew how customers navigated through the store, how they were influenced by promotions, reviews, and what others did. Predicting which book will be read next or what customers can be influenced to buy no longer belongs in a work of science fiction. Storing and analysing customers' reactions to recommendations enable all sorts of personalization strategies, and may open application of sales methods leading to sales not in the interest of buyers. In 2005, companies were collecting data, but made little use of it since they lacked the technical means and the analytical knowledge to do so. Around 50% of German companies gathered information about purchase and payment histories and used information for personalization and individualization efforts during contact to customers. Only 11% collected data automatically and more than 90% gathered data without the help of service providers, but also confessed to having no strategy of how to exploit data[128]. Today, technology for data collection is available both in terms of the architecture of support services as well as in terms of the hardware and software needed. Data-centric e-commerce came about because of three technical advances:

- Volume: As of 2012 about 2.5 Exabytes are generated every day, and this figure doubles approximately every three and a half years[129].
- Velocity: For many services in e-commerce speed is more important than volume. For instance, access to mobile phone location data combined with shopping records may give a better prediction about sales in a shopping centre. Algorithms will, for example, track types of clients from cars parked on a parking lot at a particular moment in time, and make inferences from this knowledge about expected sales.
- Variety: Big Data draws patterns from all sorts of structured and unstructured formats including textual messages, audit data or images. Data is received from sensors or GPS signals, from cell phones, or gas stations when a digitized form of payment is used. Many essential forms of data collection are new, e.g. Facebook is just eight years old, Twitter six. Enormous streams of data are tied to people, activities, and locations, and finally to product and services sales.

While in classical and cooperative e-commerce, complexity transformed security and privacy to non-technical barriers in the competition for uncommitted buyers, in the data-centric stage of e-commerce, willingness of buyers and contributors to participate and leave personal data is the deciding factor between sellers' ability to succeed and society's ability to generate increased productivity. On one hand trust can reduce search costs (e.g. because a buyer does not need to compare an offer with several others), on the other hand it increases

125 McAfee/Brynjolfsson 2008.
126 Brynjolfsson et al. 2011.
127 Buchmann 2012, pp. 143 - 188.
128 Sackmann/Strüker 2005.
129 McAfee/Brynjolfsson 2008.

switching costs and decreases capabilities to change sellers. The means to balance trust and privacy is not secrecy, as proposed by PET (privacy enhancing technology) but by transparency and the TET (transparency enhancing technology). Monitoring and Dashboards are the instruments and technologies of data-centric businesses to increase transparency, and act as both a signalling and a screening tool.

Crowdsourcing

The concept of crowdsourcing[130] allowed for the emergence of new kinds of collaborative products, services and information retrieval channels, such as open source software, online encyclopaedias (e.g. Wikipedia), digital cartography (e.g. OpenStreetMap), restaurant quality ratings, or location-based services, or statistics about hardware and software usage[131]. At first glance, the benefit is to the supplier who outsources costs. However, closer examination reveals that the consequences for the relationship and market balance can only be judged when one side becomes dependent upon the other.

OSNs and mobile apps as CRM

Online social networks and businesses' own mobile applications[132] (e.g. Amazon's Windowshop, Mercedes-Benz Service app) open new ways of marketing, advertising and communicating with and amongst customers. They play an increasing role in terms of customer relationship management, as they allow for personalized and context-dependent offerings. In terms of OSNs, the advantage for sellers is that users trust their friends and like-minded contacts. Products being advertised through friends are likely more relevant for buyers' decisions than advertising without personal context.

Aggregation and optimisation

In data-centric e-commerce, the development costs and the design of e-markets depend firstly upon the chance to incur switching costs and secondly on the technology to allow this at the lowest cost possible. Cloud computing comprises the aggregation of all kinds of services at extremely low cost. Nowadays services can be delivered to end users by means of cloud computing[133]services, mobile and desktop apps, or a combination thereof. Marketing terms such as PaaS and SaaS (Platform/Software-as-a-Service[134]) promise easy access for any number of users at the same time. All of these services depend upon the availability of cloud computing.

Cloud computing and its additional service offerings have formed specific contexts. Ambient and pervasive computing extends this rather simple understanding of context to individually preferred contexts. Here, context is an individually predefined subsection of the real world. In ambient and pervasive computing appliances[135], sensors, software, and embedded systems are windows to the real world providing real time data at any time. Automobiles, for example, are equipped with sensors, making it possible to report problems and failures immediately or even before components actually break. Printers can detect when they run out of toner, manufacturing lines report that they are running out of certain resources, and estimate production times depending on contextual information such as workload, order logs, or traffic conditions. Mobile devices can be used for immediate payment in conventional stores such as Starbucks[136]. Combining this technology with other technologies such as RFID may eventually eliminate the need for cashiers.

130 Leimeister et al. 2009, pp. 197-224.
131 Steam 2013.
132 Ibach/Horbank 2005, pp. 134-147.
133 Müller et al. 2011, pp. 129-131.
134 Weinhardt et al. 2009, pp. 391-399.
135 Augusto 2007, pp. 213-234.
136 Miller 2012.

Future autonomous computing[137] appliances will take these developments even further. Web services for personalizing and ordering products (e.g. car customization) will be connected to the corresponding manufacturing lines and will be able to instantly calculate delivery times and prices – depending on current manufacturing lines' contextual information. The manufacturing process would then, for example, be automatically begun just after the consumer submits the order online. Business intelligence will optimise the workload of manufacturing lines and initiate the delivery process to the customer as soon as production has finished. Instant payment services allow for continuously charging customers, therefore abandoning both pre-payment and post-payment in favour of in-time-payment. Future dashboards will not only be web-based but also accessible by mobile devices as well as embedded systems.

One of the great barriers for European and international e-commerce is still its legislative weakness, effectively hindering consumers' trust in cross-border shopping. This includes the handling and usage of data collected by the support service. No customer is capable of judging the possible legal or other consequences of her future behaviour.

4.2 E-COMMERCE FROM THE LEGAL PERSPECTIVE

While the co-evolution of technology and markets leads to today's different co-existing forms of e-commerce, societal interrelationships increase and call for the public stakeholders to regulate differing interests. Due to the trend towards data-centric business, data protection regulation is one option to balance markets. The objective from a legal point of view is to contribute to the undisrupted development between the technological push, the market pull and the public interest. Since data protection laws and principles exist, the pressing question is, whether the regulation has kept pace with technological and economic development, and what options for an extension of the co-evolution involving regulation should be imagined. With regard to e-commerce, legal regulation has two objectives: (1) Maintaining user privacy to the highest degree possible, while not hindering conclusion of binding contracts and correct execution of these contracts. All stakeholders must be considered equally when setting out principles for private data management. (2) General provisions like contract law, protection of minors, consumer rights, penal law, copyright law and competition law must of course be observed in e-commerce, as anywhere else.

On the EU-level, provisions of web shops and communication in e-commerce are regulated by the "E-Commerce-Directive" (ECD)[138], the "Data Protection Directive" (DPD)[139] and the "Directive on privacy and electronic communication", (DpeC)[140] implemented in Germany by the Telemediengesetz (TMG), Telekommunikationsgesetz (TKG) and the Bundesdatenschutzgesetz (BDSG). The "E-Commerce-Directive" contains requirements for "information society services"[141] concerning transparency in e-marketing and e-communication and for the liability of service providers. The "E-Commerce-Directive" has been implemented in Germany by the TMG. Information Society Services are treated as telemedia services. Telemedia services are all electronic information and communication services, which are not telecommunication or broadcasting services, e.g. search engines, social networks, online games, blogs and online newspapers. Many "e-commerce" services fall under this category, e.g. webshops, auction platforms, or app-stores.

The E-Commerce-Directive guarantees the general freedom to provide information services between EU-Member States

137 Sterritt 2005, pp. 79-88.
138 EU Directive 2000/31/EC.
139 EU Directive 95/46/EC.
140 EU Directive 2002/58/EC.
141 EU Directive 98/34/EC: " 'service', any Information Society service, that is to say, any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services."

and provides the basis for such services to be set up in other countries without prior authorization. The directive also establishes which data a service provider needs to provide about the organisation and about the service. Furthermore, unsolicited commercial communication needs to be identifiable as such. Fundamental privacy principles are valid for all "e-commerce"-services, regardless of whether they fall under the DPD/TMG as "Telemedia Services" (e.g. auction platforms, online shops, and teleshopping) or under the Dpec/TKG as "Telecommunication Services" (for example contracts concluded by mail). These principles are the concepts behind all data protection regulations throughout Europe. Moreover, these principles are the standard for judgement of whether an existing legal regulation encourages privacy with respect to technology and economy or needs to be adapted and reformed.

A lawful processing of personal information requires either a permit by legal provision for the specific processing or the informed consent of the data subject. According to the principle of purpose, personal data may only be processed for previously defined purposes.[142] The principle of necessity states that whenever personal data is processed only the data may be processed which is necessary and only as far as necessary to achieve a specific purpose.[143] For example §§ 14 and 15 TMG and §§ 28 ff. BDSG clearly state for which purposes the aggregation of users' data is allowed. This limits service providers to fulfilling contractual duties, deviating only if justified interests outweigh those of the users or if the data is generally accessible from public sources. Purpose and necessity must be transparent to the user upon request for consent as well as in the case of provision-based processing. No general data retention by service providers shall be conducted unless the legal provisions expressly provide otherwise or if the user gives his or her informed consent. Furthermore, personal data is supposed to be collected directly from the data subject, not from third parties (the principle is not contained in EU law, but for example in § 4.2.1 BDSG). Exceptions require a provision permitting or requiring that data be collected without the data subject's participation. Direct collection is supposed to support the principle of transparency and ensure the right to informational self-determination by enabling the user to exercise rights to information, correction, and deletion of personal data. The principle of data minimisation (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.

The ECD establishes that national law needs to provide provisions on electronic contracting, so that e-commerce transactions will not be hindered by legal form regulations, such as "written form". Some contracts, such as contracts concerning financial credits from suppliers to consumers, need to be in written form (signed by hand). The German Civil Code (Bürgerliches Gesetzbuch) contains a special form provision, custom-made for classical e-commerce which can replace the written form. Since written form may actually hinder e-commerce, provision of this electronic form supports e-commerce. Here, a qualified electronic signature, as defined in the Signaturgesetz, is required. Electronic signatures may be applied as a mechanism to simultaneously implement both privacy-friendliness and e-commerce-friendliness. A digital or electronic signature has a high degree of reliability, and reduces cost on the sellers' side when it comes to authentication of buyers. In addition, digital signatures promote privacy for the customer by allowing aliases. This allows the establishment of a pseudonym, which can be linked to users' proper names in the case of legal disputes, but otherwise protects the privacy preferences of users.

Since data collection and usage processing in data-centric e-commerce is automated, manual monitoring for legal compliance is virtually impossible for all stakeholders; the user, businesses, and authorities as well. In addition, monitoring of global providers by national authorities may

142 Gola/Klug 2003, p. 4.
143 Gola/Klug 2003, p. 48.

prevent opportunities and may be legally cumbersome. Thus, the concepts of *data protection by design* become very important, data minimisation being one example, but also means for users to have their privacy preferences enforced automatically.

E-commerce providers attempt to gain general consent from their users to agree to their privacy policies, which users are required to accept in order to use the service at all. These practices are often unable to produce legally-binding consent, because the policies are not specific in detail or they are too extensive to be expected to be read by users. Nevertheless, this approach is widely used and thus the (often unlawful) reality in e-commerce. This type of "consent" in the present form is not able to enable informational self-determination. Technological mechanisms which were tailor-made for classical e-commerce, like Electronic Signatures or PKI (Public Key Infrastructures), will not suffice, since they do not react to the automated and implicit processing of personal data by default. Thus, one conclusion is that even if adequate principles for privacy in data-centric e-commerce are indicated and contained in current legislation, they are not consequently carried out.

4.3 E-COMMERCE FROM A SOCIOLOGICAL AND ETHICAL PERSPECTIVE

E-commerce, like any other form of intrusive and adapted socio-technical network, has a significant impact on societies. E-commerce enables transformations of social interactions and ethical principles which do not affect all stakeholders equally. In sociological terms, this section discusses potential effects of cooperative and data-centric e-commerce on society. This will be done by focusing on the buyer's side, since here the changes usually are experienced in a more or less passive fashion.

E-commerce takes place in an e-market, and from the point of view of social theory, markets are embedded in the structured social relations that constitute society.[144] In this sense, e-commerce may be called a *reductive frame* embedded within the wider socio-technical networks of society:[145] Reduction limits transactions to their economic purpose. The other network relations are temporarily excluded and not taken into account.[146] For example, if a book lover is served by a clerk in a bookstore who happens to be the book lover's neighbour, the latter relationship is suspended, and the focus is on the relationship between buyer-product-seller. With only the economic objective in mind, a price and a contract is negotiated, with only buyer-product-seller participating in the negotiation, although society at large made such a meeting possible, and is most likely affected by the transaction.[147] E-commerce has an impact on society as a whole which means that the socio-technical relations overflow into the market frame of e-commerce. Overflow makes the emergence of markets possible in the first place, even if they are not part of market transactions as such.

4.3.1 OUTSIDE THE MARKET FRAME

The transformation of framed relations overflowing the market frame between sellers, buyers, and products are outside

144 Granovetter 1985, pp. 481-510.
145 Callon 1998.
146 Callon 1998, p. 18.
147 An example from e-commerce would be buyer 'A' who buys book 'X' on amazon.com, because X was recommended to A by Amazon on the basis of other consumers' purchasing behaviour: "people who bought book Y were also interested in book X". So, A decides to also buy X. In this case, what has happened is that the sociotechnical network of Amazon and its consumers has contributed to generate a market frame consisting of A (buyer), Amazon (seller), and X (product). In the economic transaction, it is only those three entities that interact to perform a price discovery process and to conclude a contract stating that property rights are exchanged. None of the consumers who contributed to establishing this market frame (by enabling Amazon to make a recommendation to A) is paid for its contribution; yet, without these contributions, the market frame could not emerge.

the market frame, although effects may occur inside and outside the market frame. For the domain of e-commerce it is supposed to be a technology-supported form of consumption. In social theory, consumption is more than the satisfaction of existential or purely functional[148] needs; instead, classic consumption is attributed to a process of distinguishing oneself from others in order to create a self and attain a specific social position.[149] Owning something is interpreted as disposing of symbolic capital, signalling belonging to particular social strata.[150] Consumption, understood in this way, attributes some kind of cultural significance to specific products, i.e. sneakers signalling membership in a certain sub-culture or cars symbolizing membership in a well-off social circle. Furthermore, consumption is about the generation of a manifold of social relations, (e.g. when purchasing things, trying on new outfits, talking about shopping with peers, being advised by clerks etc.) within which interplay between selves and others occurs and relations are established that go beyond the basic purpose of purchasing. Via consumption, selves strive to become desirable to fellow human beings. For this purpose, consumers put themselves in the position of those fellow beings, i.e. the "generalized Other"[151] in order to gain insight as to how to appeal to others. This generates relationships with those others.[152]

The process of creating a self becomes formalized and the identity of a consumer is subsumed under a category. For example, an e-commerce seller wants to portray a buyer as a type of shopper with specific preferences, and represents said buyer using bit strings within a known category of the cyberworld that marks who that buyer is in a given market frame. For example, cooperative e-commerce might serve as an opportunity to find social appreciation via casting oneself as price-conscious consumer.[153] Taking this observation to its limits, cooperative e-commerce can mirror the unstructured modern self, namely, when consumption is not concerned with meeting existential or purely-functional needs, but rather self-referential taking pleasure in pleasure. Consumption associated with cooperative e-commerce allows the establishment of social relations, but also serves the simultaneous purpose of distinguishing oneself from others, while networking with others to get cheap, quick and easy access to rare products; to compare prices; to discuss product quality and advise each other or be personally advised and addressed by suppliers[154].

4.3.2 WITHIN MARKET FRAME

Whereas users/consumers, computers, servers, the Internet etc. build the societal networks within which e-commerce markets are embedded, the interplay and relations established among all these entities also transform the market from within. Transformation of framed relations between buyers, sellers, and products are triggered by the unique and new feature of e-commerce as compared to classical commerce. Because an economic transaction deals with digital "things", it allows user participation. As a result, consumers tend to be more tightly integrated into the production and marketing process. Such integration might occur with the knowledge of consumers; however, it also occurs when consumers unwittingly provide data, e.g. receiving cookies from DoubleClick when interacting with Amazon allowing retailers and online advertisement firms to fuse market research and marketing. The interrelationship of buyers and sellers has exceeded the set market frame, which in

148 For the sake of brevity, we omit an extended discussion on the problematic of terms, such as "existential" and "purely functional."
149 Hellmann 2005, p. 13.
150 Bourdieu 1982. Especially in affluent societies, participating in consumption is strongly related to social inclusion/exclusion, see Lamla 2011, p. 96; see also Bauman 2009.
151 Mead 1934.
152 Miller 1998, p. 148.
153 Lamla 2012, p. 10.
154 Consumers increasingly expect offers to be submitted in a "personalized" way (Meißner 2008, p. 162).

a long run demands a more equal distribution of benefits between buyer/contributor and seller.[155]

The transformation enabled by cooperative e-commerce also affects the products offered, as said products become less pre-determined. This is due to:

(1) the opportunity for consumers to effectively influence sellers;
(2) an increase in the quantity of suppliers and of products participating in market.

This lays the groundwork for the emergence of niche markets, i.e. of markets offering products rarely asked for and rarely sold.[156] Appearances of niche markets are also shown in "longtail" markets, in which falling demand of products requires new involvement of consumers, e.g. by projecting a specific self in the product. Longtail and niche markets generate a hierarchy within the market frame, where profitable sellers coexist with "small", less influential shops. Simultaneously, the range of products offered becomes more heterogeneous, where consumption has an opportunity to escape from the commodity offerings[157] and generate a global or ubiquitous set of complex preferences[158]. The global scope of cooperative e-commerce is governed by dominating intermediaries, offering information and access to certain preferred contacts of customers. From a social theory point of view, such intermediaries can be understood as "obligatory passage points" (OPP), i.e. as actors that manage to build a network in which they take a central position allowing them to capitalize on the diverse interests of, and to shape the behaviour of a manifold of actors.[159] So far, the e-commerce intermediaries have not taken advantage of their OPP position by raising prices. This raises a question that is of utmost importance for ethics, social theory and economics alike, namely the question of guaranteeing fair and diverse market relations.

4.4 THE BENEFITS OF E-COMMERCE

The term "benefit" suggests the existence of a provision list showing the effects of e-commerce on society. This deterministic view is far from reality. E-commerce is driven by public interest, and the options available result from market opportunities, which may have side effects requiring further regulation. What might be beneficial to one member within a group of stakeholders may be considered negative for another[160]. Consider the indisputable increase of productivity and cost reduction as well as product availability worldwide: for some, a sign of increased freedom of choice and participation while others may consider this an indication of a wasteful exploitation of resources, including taking advantage of willing volunteers. In this chapter, the discussion of the benefits of e-commerce happens in reference to a European view of some core values: (1) free self-determination, (2) democratic participation, and (3) economic well-being. Nevertheless, the following view originates from the buyers' side. In order to address the supply side the changes in market design are drastic. For example, suppliers wish

155 It is still open to question whether the escape of the overflowing relations from the economic transaction of the market frame brings about negative externalities (the production of economic costs not appearing in the frame of the economic transaction), and thus causes damage for societal economy as a whole by inducing information deficits on the consumers' side (information asymmetry). *If* this proved true, the costs produced by the information asymmetry would then have to be re-integrated into the economic transactional (or market) frame, in a similar way as, say, the costs generated by fumes have been re-integrated into the market frame via emissions trading (see Chapter 7 'Constructing Emissions Markets' (MacKenzie 2009). Moreover, if the information asymmetry thesis is correct, Internet privacy can be considered an antidote to the emergence of the asymmetry.
156 Anderson 2006.
157 Meißner 2008, p. 161.
158 Schelske 2008, pp. 186-188.
159 Callon 1986, pp. 196–233.
160 Buchmann 2012, pp. 15-62.

that each user has economic ownership of his or her data, which can be sold to data collectors and the user receives a license fee, when the data is used. A second condition to ease suppliers' burden is to give up privacy completely, and install an investigative institution to handle cases of unfairness. The concept used here focuses on the demand side, where a lack of market transparency generates information deficits[161] and in the long run endangers innovation e.g. by potentially increasing inequality[162].

4.4.1 THE BENEFITS OF E-COMMERCE FOR FREE SELF-DETERMINATION

E-commerce and free self-determination have a relationship with regard to the following four conditions:

1. Development of a self.

2. Free interaction with others. This encompasses the decisions with whom to interact, what portions of the world one incorporates into oneself, and how much information one wants to allow others to have about oneself.

3. Free embedding in a society. There is no free interaction without being embedded in a society. Society gives space and rules to act.

4. Conviction that the picture about oneself is identical to the pictures others have.

Development of e-commerce has three phases, whereas the classical stage offered the choice to buy or not to buy. The cooperative phase allowed the participation of buyers and the current data-centric phase gathers information about social relations. "Consumption" becomes the means of free self-determination, in an effort to synchronise the image one has of oneself with the image which is perceived by others. Whereas the development of a self requires freedom of choice, free interactions are improved by e-commerce.

Increasing the number of options for product selection

E-commerce promises to make items and services available from all over the world, thus massively expanding the range of commercial options one can choose from. Another positive aspect is the abundance of options provided by the storage of customers' search and order histories on e-commerce platforms. Purchasing books on *amazon.com* is a case in point, for the storage and smart correlation of information concerning goods purchased in the past to suggest consumers similar products to be purchased in the future. This correlation increases the number of viable options that a self might consider[163] – options that one would otherwise have to self-generate by investing considerable effort and time into researching those alternatives.

Improving convenience, ease, and comfort of shopping

Another benefit of e-commerce is that it brings about the possibility to search for, evaluate, select, and purchase goods and services from home. The ability to determine the time and date of the purchase provides more options for time management, e.g. taking care of the shopping on Friday evening allows families to spend more time together on Saturday.

More options for self-expression

E-commerce provides new opportunities for self-expression, in a semiotic as well as in a material way. As far as the former is concerned, consumers may not only buy goods but may also deliver an assessment of the product's and supplier's performance afterwards, thereby expressing their

161 Meißner 2008, p. 158; Schelske 2008, p. 170.

162 Meißner 2008, p.186.

163 It has to be noted, though, that there exists a type of consumer who disapproves of the submission of such options. Consumers who follow an internal "relevance hierarchy" tend to conceive of alternative offerings as a manipulative attack on their autonomy, severely restricting self-determination. Lamla 2012, pp. 6-8.

experience. Moreover, those statements can be viewed by others and thus become helpful information for making future purchase decisions. As far as the material way of self-expression is concerned, some suppliers have interactive tools available to self-design products, especially fashion products, such as T-shirts, sneakers etc.

Prosumers: Consumers becoming suppliers

Finally, e-commerce not only provides a multiplicity of opportunities for entrepreneurs to develop innovative business models. The opportunity to develop new business models contributes to self-determination. Consequently, e-commerce also improves self-expression by reducing the obstacles users face to run a business and become entrepreneurs.

4.4.2 THE BENEFITS OF E-COMMERCE FOR DEMOCRATIC PARTICIPATION

The interrelationship of democratic participation and e-commerce is to be seen in e-commerce's contribution to productivity, which as a consequence increases material wealth, which is a prerequisite of democratic participation:

1. Democratic participation is only possible if actors have the opportunity to engage in social interactions, and to materially benefit from these interactions. While social exclusion is a multi-dimensional aberration, often it goes hand in hand with economic exclusion.[164]

2. Knowledge of the rules of democratic participation is essential in order to exercise and to transform the rules. This includes active and passive rights, e.g. to vote and to be electable, and the freedom of selection to choose one's representative.

3. Democratic participation requires several types of freedom: freedom of speech and thought, as well as freedom of information, the right to assemble, i.e. the formation of organisations, communities and social relations.

Access to material wealth

Engaging in and benefitting from social interplay constituting the common good depends on access to material products and services. Kronauer clarifies that participation has a material, political-institutional, and cultural dimension[165], and it is easy to see that every citizen needs to have at least some access to the material goods produced within society to gain the freedom which democratic participation requires. Additionally, political-institutional participation to a certain degree presupposes access to the material wealth of a society, because possession also functions as a key to social networks[166].

Lowering costs: Access to public and other services

E-commerce promises to increase opportunities for less affluent people to purchase as yet unreachable goods. By raising their standard of living, the opportunity to get involved democratically may generally prosper, but also in regard to the definition of e-markets. Firstly, there is a wider range of products to be found online, and secondly, it is possible to compare prices of various suppliers. As there are more choices, one can decide on a product with better features at a more competitive price. The resulting lower costs improve access to goods and thus participation. Thirdly, people might benefit from e-commerce as the latter facilitates the delivery of public and other services. For example, some information is sent out electronically instead of on paper, e.g., bills and invoices but also newspapers, which decreases costs and thus makes some services available for people otherwise excluded from the service.

164 Bauman 2009.
165 Kronauer 2010, p. 147.
166 Hellmann 2005, p. 13.

Facilitating access to market information

More accurate information about products, which in turn allows consumers to make informed decisions, increases judgment capabilities and expands knowledge about the rules of how an economy or a democracy works. If it is true that more information leads to greater confidence when making a purchasing decision, e-commerce indeed strengthens consumer protection. This is, however, not the only way e-commerce might aid the problem of the information asymmetry, in addition, political decisions and their global interrelationships may be better understood, due to greater access to information. Consumers who cannot network in person can now build communities whose members mutually inform each other. In this sense, social commerce might increase the role played by the consumer and democratize access to market information.

Democratizing access to educational and informational goods and services

In the ideal version of democracy, each citizen has the opportunity to take part in the political formation of will and in decision-making actively or passively. In order to achieve a perfectly democratic procedure of will-formation, citizens must have access to information and must be able to receive various opinions staged through public discourse. E-commerce could possibly function as an antidote to commercialization pressures by making instruction media less expensive, and by uncoupling teaching and learning from a fixed locational setting. Thus, as e-commerce has the potential to contribute to lowering media costs and making media more widely available in electronic form, it might contribute to democratizing access to information and knowledge, and thus improve democratic participation (albeit indirectly).

Community building

Having access to a commercially motivated infrastructure allows people to also use these infrastructures for non-commercial purposes, e.g. for community buildings or democratic activities. Various online media e.g. Blogs, Chat rooms, Wikis, are becoming knowledge-sharing resources, which allow people to discuss their opinions and access information. Many of these communities are based around a single topic, often highly cooperative and sometimes establish their own unique culture giving them impact if an interrelationship to the outside world exists. Community building may democratize participation.

4.4.3 THE BENEFITS OF E-COMMERCE FOR ECONOMIC WELL-BEING

Well-being in a German context describes the effort and potential to strive for a "fair" and "equal" distribution of wealth produced by the society as a whole. This is different from other societies, since concepts such as "fair" and "equal" are determined in a profoundly normative way. Some recent definitions include life satisfaction or experienced benefits. In a European context, however, well-being describes the societally-accepted form of income distribution between all members of society.

Benefits for customers

The main benefit for buyers is their improved capability to identify fitting products and services at any convenient time. These are two aspects of market transparency: aggregation of individual economic activities, and generating informed consumers/businesses.

Aggregating individual economic activities and rendering them visible (market transparency)

While economic transactions between individual sellers and buyers hitherto have been accomplished locally and rather randomly, ebay.com serves as an umbrella that removes transactions from a locality and opens up a wide range of searchable offers. This leads to an increase in economic transactions and to an aggregation of individual transactions, with the effect of wealth being generated.

E-commerce enables the most efficient pooling of supply and demand. By making this visible, the market becomes more transparent. Due to increased transparency, markets and the allocation of resources become more efficient, increasing income generation and options for distribution.

Generating informed consumers and businesses (market transparency)

Unless competition and freedom on the Internet is systematically restricted, e-commerce allows for the provision of information to economic agents to make free and rational decisions. Economically relevant news and even the atypical agents who act in illegal or unethical ways become the focus of public attention easily. In this sense, product and service quality is subject to a form of socio-economic self-control, which adds trust, and reduces faulty purchases. It is technically possible to create a global community of informed consumers and businesses. Cooperative e-commerce is more efficient than social commerce.

Benefits for businesses

Businesses or sellers need to increase their understanding of customer preferences as well as communicate with other businesses. In business communication, the exchange of information is necessary due to transactions occurring in phases, resulting in increased cooperation to achieve an objective. Regarding communication with customers, the reduction of search and switching costs is critical.

Communication within and between businesses

The Internet also plays an important for internal processes: 78.0% of companies claimed in 2005 they used the Internet for internal communication. The main goal by doing so is to increase efficiency. The Internet is used in a similar manner to connect businesses with other businesses' information systems (45.7% claimed to do so in 2005). 63.4% stated they planned to intensify these kind of connections.[167]

Communication to customers

Any business that expects to grow profitably and effectively will have to master the art of selling through e-commerce channels. Today, technology is available to fit both product design and e-commerce channels. This growth requires business analytics and customer involvement to either enhance the capability of existing channels and/or to identify at a very early stage which channel is the most appropriate for a product. In classical commerce this knowledge was incorporated into the seller's cognitive capabilities. Today, such customer relation practices are global and thus more predictable and fair.

Public administration

Public Administration services are most often referred to as e-government but can also be seen as C2A (Customer to Administration) e-commerce. The motivation of e-government is not to increase profits, but to add to the convenience of citizens, to lower the costs of a list of services, and to enable a more efficient administration[168].

Benefits for both customers and businesses

Besides being a channel of distribution, the Internet also became the most important communication channel between customers and businesses. In 2005, 89.9% of German companies could be contacted online, and 91.6% presented product information online. Almost one out of three businesses (33.1%) used online advertisement to foster sales. The Internet has an impact on customer behaviour: 48.4% of businesses claimed that customers often referred to information given online. The majority of businesses did not use different pricing models for offline and online sales in 2005; only 27.7% claimed to use more flexible pricing online. Customer data is of great importance: Even in 2005, 65.2 % of businesses stated that they collect and analyse customer data. Payment history and buying behaviour were of special interest. The main purpose of this data was to

[167] Sackmann/Strüker 2005.

[168] Müller et al. 2011. Only a few of these services are available to citizens and are implemented on the E-Identity card. One reason is unresolved privacy issues.

address customers more personally, e.g. through advertisement (for 57% of businesses that was a goal). About 30.7% of businesses also stated data was used to optimise internal processes, e.g. by making better strategic decisions based on customer data. The collection of customer data has become steadily more important since then.[169]

Globalization of markets for all

E-commerce further accelerates the "Globalization of Markets" already having been diagnosed in the early 1980s[170]. The first sentence of T. Levitt's paper reads: "A powerful force drives the world toward a converging commonality, and that force is technology. It has commodified communication, transport and travel. It has made isolated places and impoverished peoples eager for modernity's allurements. Almost everyone everywhere wants all the things they have heard about, seen, or experienced via the new technologies. The result is a new commercial reality".[171] E-commerce further transforms this reality by continuing to extend markets insofar as more suppliers have the chance to sell more and diverse products.

Reaching narrow, specialised, and niche markets

The process of extension goes along with an increase in the accessibility of rather small markets. Whereas a classic retailer, due to the limitations of space is only able to offer a limited range of products, e-commerce businesses can also offer goods rarely sought: "The era of one-size-fits-all is ending, and in its place is something new, a market of multitudes"[172]. Businesses, such as Amazon, for example, are able to capitalize on the long tail products, "Our culture and economy are increasingly shifting away from a focus on a relatively small number of hits (mainstream products and markets) at the head of the demand curve, and moving toward a huge number of niches in the tail. In an era without the constraints of physical shelf spaces and other bottlenecks of distribution, narrowly targeted goods and services can be as economically attractive as mainstream fare"[173].

169 Sackmann/Strüker 2005.
170 Levitt 1984, p. 2.
171 Levitt 1984, p. 2.
172 Anderson 2006, p. 5.
173 Anderson 2006.

5 PRIVACY THREATS AND THEIR IMPACT ON THE CORE VALUES

In Chapter 4 we discussed many ways online social networks and e-commerce support the realisation of the core values which guide our normative approach, introduced in Chapter 2. However, the benefits of OSNs and e-commerce are also accompanied by threats. In this chapter we investigate potential privacy violations in OSNs and the consequences they might have for the core values. We start by analysing OSNs. First we present central conditions whose fulfilment provides privacy protection in OSNs. In order to evaluate the threats to privacy in OSNs we analyse when and how these conditions may be violated. This is the purpose of the second section in this chapter. In the third section, we explain how a violation of the central conditions and thus a loss of privacy in the context of OSNs can negatively impact our core values: free self-determination, democratic participation, and economic well-being. We then show that the analysis of OSNs to a large extent also applies to e-commerce and mention additional aspects that are relevant for e-commerce. We will conclude that the privacy conditions need to be fulfilled as far as possible in order to safeguard our core values.

5.1 CONDITIONS FOR PRIVACY PROTECTION IN OSNs

Analysing existing legal frameworks for data protection and privacy protection principles from the relevant literature[174, 175, 176, 177, 178, 179, 180], we have identified three conditions which have to be fulfilled in order to gain privacy protection in OSNs. These conditions are *awareness, control,* and *trustworthiness*. OSNs deal with personal data of their users. In accordance with the EU Data Protection Directive[181], personal data is defined as "any information that relates to an identifiable, living individual"[182]. This includes data that is collected directly and data that is derived from information processing. OSNs deal with this data according to their policies, a set of explicit or implicit rules. For example, these policies refer to the collection, processing, disclosure, and retention of personal user data. Privacy protection requires these policies to be in accordance with applicable laws and regulations as well as user privacy preferences which may vary between users or user groups. The formation of privacy preferences requires user *awareness* of the privacy-relevant aspects of these policies and their potential impact on the core values that were identified in Chapter 2. Next, the implementation of their preferences requires the users to be able to appropriately *control* the policies and related processes in OSNs that deal with their personal data in such a way that they respect their privacy preferences.

As OSNs are very complex systems, user awareness and control can only pertain to certain aspects of the OSN policies that are then customized for individual users or user groups. In addition, a base level of privacy protection must be guaranteed for all users without requiring user awareness or user control. Said base level can be achieved if appropriate (legal) regulations are in place and if the OSNs comply with them. Again, because of the complexity of OSNs, users are unable to verify that OSNs respect these regulations. So *trustworthiness* of OSNs in regard to compliance with the applicable regulations is required. In addition, trustworthiness also refers to the user preferences being respected by the OSNs, as this may not be

174 EU Directive 95/46/EC.
175 E.g. Telemediengesetz (TMG) Telekommunikationsgesetz (TKG) and Bundesdatenschutzgesetz (BDSG).
176 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) 2012.
177 OECD 2013.
178 OECD 1999.
179 FTC 2012.
180 FTC 1998.
181 EU Directive 95/46/EC.
182 EU Directive 95/46/EC.

verifiable directly by the user. So we see that the coexistence of awareness, control, and trustworthiness allow for adequate privacy protection in OSNs.

5.1.1 AWARENESS

Awareness refers to the users knowing and understanding which personal data about them is available to the OSN, what is happening to this data, what the relevant legal regulations are, what the impact of OSN data management on their privacy and the core values may be, and how they can influence this data management. Such awareness enables the users to develop and implement their privacy preferences in OSNs.

As mentioned above, OSNs deal with personal data according to their policies, e.g. for collection, processing, disclosure, retention, and the support of third party applications. By choosing their privacy settings, users can adapt these policies to their own privacy preferences. Awareness refers to the user's knowledge and understanding of the relevance of these policies and the implications of various privacy settings in order to safeguard privacy and the core values. As policies may change over time, user awareness must continue to develop with these changes. More precisely, awareness with respect to OSN policies refers to the quality and quantity of personal data collected by and available to the OSN provider and the audience to which the user data within the OSN is visible. This information includes data that the users have explicitly provided to the OSN and data that is collected implicitly. For example, the users may explicitly provide their gender to the OSN and in the interaction with the user, the OSN may implicitly record the user's IP address. Next, awareness with respect to the OSN's policies refers to the users knowing how the their personal data is handled by the OSN, in particular, how it is processed, to whom and under which conditions the data is disclosed, whether the data is modified, and for how long and in which condition the data is stored by the OSN provider. In fact, data processing may create new personal information about users. For example, in the GAYDAR experiment an MIT research group showed how to deduce the sexual preferences of users from information available about them on Facebook.[183] Also, awareness refers to OSNs allowing third party applications to run and collect data in the OSN context. This awareness includes the users knowing how to influence availability, processing, and disclosure of their personal data and to control third party applications by choosing appropriate privacy settings. Furthermore, user awareness refers to the users knowing how far they can justifiably trust the OSN to respect their privacy preferences, to obey the applicable regulations, and to deal appropriately with privacy threats. For example, this refers to the user being able to trust that corrections and deletions are performed by the OSN provider as requested.

5.1.2 CONTROL

Once users have developed their privacy preferences in OSNs, it is essential that they are able to implement them. This requires the users to have appropriate control over the OSN policies with respect to their personal data. Such control has several aspects.

The first aspect refers to the users being able to give and cancel consent for data collection, processing, and disclosure to third parties. For example, if users have given consent to sharing their data with a partner site they must be able to withdraw this consent and thereafter no personal user data may be shared with the partner site. In fact, "informed consent" is required, which means that a user "understands the nature of the information and consents to it being received, stored, processed, and analysed with [the users] knowledge for a specific purpose, and possibly for a specific duration"[184].

[183] Schroeder 2009.
[184] Krishnamurthy 2010, p. 66.

A variant of this aspect is the possibility to use OSNs anonymously or under a pseudonym, for example when users participate in a political discussion without being identified.

The second aspect refers to the users being able to access, modify, and delete their personal data in the OSN or to having it modified or deleted upon request. This includes determining to whom and for how long personal data is visible, in other words to segregate different audiences and contexts, and to limit the retention time. It even includes being able to delete all personal data in one OSN and move it to another OSN.

The third aspect of control refers to users being able to restrict third party applications which are run in OSNs and the collection of their personal data by these third parties.

5.1.3 TRUSTWORTHINESS

The OSN provider must be sufficiently trustworthy to implement an appropriate level of privacy protection, taking into account legal and social norms and user preferences. This trustworthiness has several aspects.

First, existing regulations must provide an appropriate level of privacy protection. This is not obvious since technological development is very fast and it is difficult for law makers to keep pace with this development. Also, in different countries there are sometimes many contradicting approaches to privacy protection.

Further, OSNs must be relied upon to collect, process, disclose, and retain personal data in accordance with the users' privacy preferences, social norms, and the applicable regulations. We present a few important examples for such norms and regulations to illustrate the complexity of this issue. In OSNs personal data is collected and retained for a certain purpose which is agreed to by the user or permitted by law. For instance, using OSN data for targeted advertising is a purpose to which users have agreed by signing up to the OSN. *Purpose binding* requires the OSN providers not to use the data for other purposes unless approved by user consent or by a legal regulation. A related requirement is *context binding* which means that personal data may only be visible in contexts agreed to by the data subject or justified by legal regulations. For example, a user may not want religious or political information to from her private peer group to be known in the context of work.[185] Another example is *data minimisation*[186] which is required by German law. It means that OSN processes gather and process no more personal information than absolutely necessary for their purpose. For example, playing online games within the OSN environment does not necessarily require the knowledge of user identities. Yet another example is the requirement of *context segregation* by partitioned data storage for different purposes. Regulations may also refer to the interaction of OSN providers with users. For example, when data about a user is collected from somewhere/someone else, the EU DPD requires the data subject to be notified about the data collection details such as the categories of collected data and the purpose of the collection.[187]

Finally, OSN providers must be trusted to establish a level of *security* that protects the personal data of the OSN users. Even if OSNs respect all applicable regulations and user preferences, they may not use appropriate technology to protect the personal user data that is entrusted to them. For example, protecting personal user data may require encryption. However, encrypted data is much harder to process which may deter OSN providers from using it.

However, trustworthiness does not only apply to the provider of OSNs, but also to the behaviour of other users. In

185 Wang et al. 2011, p. 5.
186 Roßnagel 2011.
187 EU Directive 95/46/EC.

order to trust that their data is safe on OSNs, users must be able to rely on their friends and other users not to distribute personal information or photos which the respective user wants to remain private or available only to a specific selected audience. Users should be able to trust other users not to violate their privacy, regardless of whether this happens on purpose or involuntarily. The desire for trustworthiness of other users can be referred to as social privacy as opposed to institutional privacy.[188]

5.2 THREATS TO PRIVACY IN OSNs

In Section 5.1 we presented three conditions that allow for privacy in OSNs: user awareness, user control, and trustworthiness of the OSN provider. In this section we discuss threats to privacy in OSNs. They become possible because 1) awareness, control, and trustworthiness are currently unsatisfactory and 2) the circumstances for the fulfilment of these conditions are not yet optimal. Analysing the current situation in OSNs and the literature[189, 190, 191, 192, 193] we have identified three main threats. The first threat is *re-purposing* and *decontextualization* which means that personal user data becomes available and is used in contexts not agreed to by the user or justified by law. The second threat is data *persistence* which refers to data being available beyond the time intended by the user or by law. The third threat is user *tracking* and *re-identification* which refers to reconstructing the association between a person and anonymous data.

5.2.1 THREATS REGARDING AWARENESS

As explained in Section 5.1.1 the condition awareness in OSNs has two aspects: awareness in regard to the OSN policies and awareness in regard to the trustworthiness of the OSN. In regard to policies, it appears to be very difficult for users to have sufficient cognizance of which personal data is collected, what may happen to the data, and what the impact of this data management on their privacy may be. For instance, users may not know that in addition to the data that they intentionally submit to the OSN, they unintentionally leave traces that add to the personal data collected by the OSN[194, 195]: websites visited, applications used, friends followed, videos watched, messages written and deleted. Users may not be aware of the access patterns in OSNs, for example when they invite people to parties.[196,197] Users may not know in which ways their personal data is disclosed to third parties that, for example, offer games such as quizzes in the OSN context. Such applications may collect and use personal data.[198] Users may not know in which ways OSNs process their data in order to derive more information. For example, friend recommendation in Facebook is based on "mutual friends, work and education information, networks you're part of, contacts you've imported and many other factors"[199], however, in many cases when a person is recommended with which the user has no common friend, nor other common information, it is unclear to the user why this person has been suggested as a friend. Users may be unaware of others revealing personal information about them by posting on their OSN page. Also, users may have insufficient knowledge

188 Raynes-Goldie 2010, pp.1-4.
189 Dumortier 2009, pp. 119-137.
190 Karr-Wisniewski et al. 2011.
191 Narayanan/Shmatikov 2009, pp. 173-187.
192 Gross/Acquisti 2005, pp. 71-80.
193 Beye 2012, pp. 87-113.
194 Northwest University 2009.
195 Howison et al. 2011, p. 2.
196 BILd.de 2012.
197 Süddeutsche Zeitung 2011.
198 Johnston 2012.
199 Facebook 2012.

regarding where and how to choose privacy settings in accordance with their preferences. This lack of awareness may lead to data becoming available and being used in contexts not known to and not agreed to by the users (*re-purposing* and *decontextualization*). In fact, currently, decontextualization appears to be the most serious privacy threat in OSNs.[200] Furthermore, users may be ignorant of the methods used to process their personal data inside the OSN. For example, users may not understand why a certain advertisement is displayed to them or why a certain person is suggested to them as a friend. Finally, users may not know how long their data is retained by the OSN providers and that it may even be kept after a user has deregistered from an OSN.[201] This may lead to *data persistence* far beyond user consent.

This unawareness of OSN policies is not so much caused by the absence of information and options for choosing privacy settings. In fact, OSNs typically provide extensive policy descriptions and such options. It rather arises because of the complexity of these descriptions and options. Also, this unawareness is caused by the complexity of the related technology that allows third parties to access personal user data, for example by cookies.[202, 203] In addition, users may not be interested in understanding policies as they do not perceive the potential implications for their privacy.

The second aspect of user awareness, users knowing that OSNs are trustworthy in the sense of providing an adequate level of privacy protection, is threatened because such trustworthiness is presently very hard to verify. Although many laws and regulations exist that require OSN providers to respect user privacy[204, 205] and numerous auditing mechanisms are applied to ensure the trustworthiness of OSN providers[206, 207, 208] most users have little knowledge about these regulations and mechanisms and cannot estimate the level of their trustworthiness. This is due to comprehensible information about laws and appropriate auditing mechanisms not being available as well as users not being aware of their relevance.

5.2.2 THREATS REGARDING CONTROL

As seen in Section 5.1.2, user control refers to users being able to grant and cancel consent to data collection and to accessing, modifying, processing, and deleting the collected data. These aspects are not yet satisfactory in OSNs.

Although OSNs do enable users to control their OSN data such as messages and photos, it has been shown by several studies that user control by means of privacy settings in OSNs is not yet appropriate as their usage is too difficult, they do not always offer a sufficient number of options, and defaults as well as options may be changed by OSN providers.[209, 210, 211, 212, 213] For example, a recent study shows that many users fail to manage their contextual

200 Wisniewski et al. 2011.
201 Europe versus Facebook 2012.
202 Turow et al. 2005.
203 Nissenbaum 2011.
204 EU Directive 95/46/EC.
205 Data subject's rights of access (§ 34 BDSG) and to rectification, erasure or blocking (§ 35 BDSG).
206 The Office of the Data Protection Commissioner, Ireland: Report of Data Protection Audit of Facebook, 2011. URL: https://www.dataprotection.ie/documents/facebook%20report/final%20report/report.pdf
207 Deloitte 2012.
208 Compliance Week 2011.
209 Krishnamurthy 2010, p. 66.
210 Liu et al. 2011.
211 Majeski et al. 2011.
212 boyd/Hargittai 2010.
213 Madejski et al. 2011.

boundaries in OSN's properly which leads to content which was intended to be visible only to certain groups such as friends or family becoming visible to others outside the designated sphere.[214] Also, there is little control of the indirect collection of personal data in OSNs. Such data may be submitted by other users, for example by tagging photos[215] or may be generated by data processing practices such as profiling (see Section 5.2.3). Indirect data collection may lead to *re-purposing* and *decontextualization* of directly collected data. In fact, data processing typically requires the input of directly collected data. But certain data processing practices may not be agreed to by the user. Also, personal data of a user provided by others may appear in contexts not agreed to by the user. In addition to the lack of control over indirect data collection and generation, the user's ability to access, modify, and delete indirectly collected personal data is unsatisfactory. For instance, data which has been submitted by users may not be removable by other individuals that appear in the photos.

In addition, user control over the retention time of their personal data, be it collected directly or indirectly, is also a critical issue. For example, according to its published policy[216] Facebook does not delete personal data such as messages and photos from their servers but makes them invisible to the users.[217, 218] This leads to *data persistence* far beyond the consent of the users. Also, because of the lack of open standards and interoperability of OSNs, users cannot move their personal data from one OSN to another.

5.2.3 THREATS REGARDING TRUSTWORTHINESS

For several reasons the trustworthiness of OSNs is still inappropriate. It is challenged as OSNs and third parties have the technical ability to collect and process personal data in many ways that may not be in accordance with the user's privacy preferences or the applicable regulations. Trustworthiness is also affected if OSNs do not properly implement IT security mechanisms that protect personal user data. However, it is not only the OSN provider's failure to implement technical measures for privacy protection which threatens the security of personal data. It can also be due to other users who share personal information or photos without the consent of the owner of that information. This may happen involuntarily as a result of insufficient awareness or on purpose with clearly malicious intent. Thirdly, regulations and auditing mechanisms, intended to guarantee a basic level of privacy protection, are not yet fully able to prevent these threats and generate trustworthiness of OSNs.

We illustrate: advanced collection and processing techniques and their potentially privacy invasive consequences. The first example is data collection by *tracking* a user's web activities outside the OSN environment such as Facebook's "Like" button, a plug-in that allows Facebook users to share their interests.[219] Another technique is *re-identification* which is possible because a sufficiently large subset of personal user data, for example a small collection of friends, is known to uniquely determine the user even if no explicit identifying information is provided[220]. This has been confirmed by several studies.[221, 222, 223, 224] The possibility of

214 Ulbricht 2012.
215 Wisniewski et al. 2011.
216 Krishnamurthy 2010, pp. 65-70.
217 Facebook 2012.
218 Cheng 2012.
219 As of 03.09.2012.
220 Buchmann 2012, p. 207.
221 Sweeney 2000.
222 Bonneau et al. 2009, pp. 249-254.
223 Bonneau 2009, pp. 13-18.
224 Wondracek et al. 2010, pp. 223-238.

re-identification interferes with the option to use OSNs anonymously or under a pseudonym. Further advanced techniques lead to re-purposing and decontextualization. Re-purposing may happen when user profiles are constructed from data that is available to the OSN.[225, 226] Profiling techniques use data collection, e.g. by log file analysis[227], and data processing such as data mining.[228] Decontextualization may happen because of inappropriate access patterns, for example, when a user's unflattering photos posted on a friend's page become accessible to her parents-in-law.[229] Decontextualization may also happen when user tags on images contain meta-data such as profiles of persons on the photo. Such decontextualization may be caused by inappropriate default settings and changes in the access rights over time[230, 231]. The latter OSN settings often go hand-in-hand with inappropriate user behaviour. Decontextualization is also caused by other users who may share images and personal data or tag their friends in photos without authorization. If there are no control mechanisms implemented by an OSN which request authorization by the data's owner, this constitutes a threat to the perceived trustworthiness of an OSN. In addition to the OSNs and their individual users, third parties that collaborate with OSNs may also apply privacy-invasive techniques to OSN user data. For example, third party apps which are offered within the OSN environment may ignore the data minimisation requirement by collecting personal data beyond any control.

The second threat to trustworthiness is caused by OSNs not properly protecting the security of the personal data of their users. For example, encryption technology may not be applied appropriately or access protection mechanisms may be insecure. Also, secure operation of OSNs requires the OSN employees to satisfy security requirements. Where there is inadequate protection, third parties have an easier time gaining access to sensitive information within the OSN.

Thirdly, today's legal regulations and auditing techniques that are supposed to prevent the application of privacy-threatening techniques described in the previous sections do not fully guarantee this. Laws and regulations do not yet reflect existing technology adequately. Even more importantly, OSNs are "global" while regulations and laws are "local," e.g. applicable only in certain countries. Different cultures and preferences may lead to variable and sometimes conflicting regulations. For example, in the U.S. data processing is permitted unless explicitly prohibited by law. In contrast, German law prohibits data processing unless expressly permitted by law. This makes it difficult for OSN providers to implement their systems in accordance with all regulations. Additionally, auditing mechanisms do not yet work as intended. They are again "local", their value is unclear, and they are not sufficiently transparent to users.

5.3 THE IMPACT OF PRIVACY THREATS ON THE CORE VALUES

In Section 5.2 we discussed threats to privacy in OSNs. As explained in Chapter 2, we consider such risks to be relevant if they have a negative impact on the core values defined there. In the following we discuss this impact. It would be desirable to illustrate this impact with relevant examples. However, we will only be able to give examples for the negative impact of the threat of decontextualization as this appears to be the most critical issue in OSNs

225 Narayanan/Shmatikov 2009, pp. 173-187.
226 Hildebrandt 2008, pp. 17-45.
227 Hancock et al. 2007, pp. 449–452.
228 Buchmann 2012, p. 236.
229 Buchmann 2012, p. 233.
230 boyd 2008, pp. 13–20.
231 McKeon 2012.

today. Nevertheless, even though somewhat speculative, we consider it important to illuminate other possibly negative effects on the core values. Such possible impact influences the behaviour of users in OSNs and may become more serious in the future. The considerations of this section will enable us in Chapter 6 to propose appropriate measures that balance the advantages of OSNs for the core values presented in Chapter 4 with the risks described in this chapter.

5.3.1 THREATS TO FREE SELF-DETERMINATION

In Chapter 2 it was explained that free self-determination requires individuals to be able to present themselves as the self they choose to be within the interplay with others. In Chapter 4 we saw how OSNs can support this requirement. However, the threats presented in Section 5.2, in particular repurposing/decontextualization, data persistence, and tracking/re-identification, can negatively affect free self-determination and, in particular, the aspect mentioned above.

Re-purposing and decontextualization can negatively influence free self-determination since both may lead to personal data being disclosed to individuals who are not the intended viewers. There are several examples that demonstrate this. In 2007 a woman claimed that her teaching career had been derailed by college administrators who unfairly disciplined her over a MySpace photo that shows her wearing a pirate hat and drinking from a plastic cup.[232] This photo was not meant to be visible in the college context. Another example is the case of Bobbi Duncan whose sexual preference was exposed to her father and 200 Facebook friends against her will when another user added her to a Facebook discussion group. As a result, her father left threatening messages on her phone.[233] A third example is the case of Nathalie Blanchard of Quebec who lost disability insurance after she posted a photo on Facebook.[234] As seen in Section 5.2, decontextualization in OSNs may happen in many ways. Users may be unaware of the context in which their personal data is visible or they may be unable to choose appropriate privacy settings. Users may reveal personal information of others as in the above example. Personal data may also be generated by data mining techniques as in the GAYDAR experiment (see Section 5.2) or collected by third parties without the data subject's consent. Again, this may lead to personal information being disclosed in inappropriate contexts. In each of these cases, self-determination of OSN users may be seriously harmed directly or indirectly. It is harmed directly, if the sharing of personal data leads to negative consequences for the user as in the above cases. Self-determination may be also compromised indirectly. The possibility of decontextualization can make users feel reluctant to make full use of OSNs[235, 236] and can prevent them from taking advantage of the positive impact of OSNs on self-determination described in Chapter 4.

As with decontextualization, the possibility of tracking and re-identification may also negatively affect self-determination. Users of OSNs may not want their whereabouts or identity to be disclosed in certain contexts. This is why they may use pseudonyms or act anonymously. However, as explained in Section 5.2, tracking and re-identification techniques are advanced, potentially making anonymous information linkable to identities. This may lead to personal information being disclosed in contexts not intended by the respective individual. Again, the negative impact on self-determination may be direct (negative consequences for users) or indirect (users becoming reluctant to use OSNs that may otherwise support free self-determination).

232 Opsahl 2010.
233 The Smoking Gun 2007.
234 Fowler 2012.
235 CBS News Montreal 2009.
236 Aberjhani 2012.

Data persistence may make the issues discussed so far even more serious. Self-determination does not refer to a process of creating a self that, once it is achieved, is settled once and for all, but to a constantly ongoing endeavour. Creating a self is a constant becoming, including the process of ongoing self-transformation.[237] Storing personal information for an unlimited time period may lead to individuals being held responsible for past actions which may interfere with their right to self-transformation.[238] This is even more critical when re-purposing, decontextualization, or re-identification is applied to persistent data.

5.3.2 THREATS TO DEMOCRATIC PARTICIPATION

The discussion in Section 5.3.1 applies equally to the core value of democratic participation. In Chapter 4, it was shown that democratic participation may be considerably supported by OSNs. However, political opinions and actions provided to OSNs or inferred from OSN information may be de-contextualized, again leading to negative consequences for the respective individuals or to them being discouraged from using OSNs in political discourse.[239, 240] Anonymous or pseudonymous participation may be of particular importance when OSNs are used for democratic participation. So the possibility of re-identification may have an extremely negative impact on democratic participation. Possible data persistence makes things much worse as the political development of individuals is typically very dynamic. Since the relevance of social networks for communication processes is increasing, the discussed threats to democratic participation in OSNs may have very a negative impact on democratic processes in general.[241]

5.3.3 THREATS TO ECONOMIC WELL-BEING

The privacy threats identified in Section 5.2 may also have negative consequences for economic well-being. A fundamental characteristic of OSNs and their business model is the collection and dissemination of data. Privacy violations such as re-purposing, decontextualization, data retention, tracking, and re-identification may lead to an information deficit on the user side: users know less about the usage of their personal data than OSN providers or third parties. Such information deficits may reduce the benefits of OSNs in three ways. First, there may be direct effects, e.g. unfair pricing since the users do not know what the value of their personal data is. Next, there may be indirect effects. For example, information deficits on the user side, and, more generally all potential privacy violations, reduce the trust in OSNs and thus the willingness of new users to join OSNs. Also, they may reduce the attractiveness of OSNs to potential professional customers, e.g. supply-chain industries like app communities. This, in turn may lead to a growth of OSNs below their potential. Thirdly, there may be induced effects. Due to privacy violations, OSNs may become less attractive as infrastructures for communication, cooperation and coordination of professional customers. As a consequence, these potential customers may experience a growth and development below their potential. Another possible negative effect of privacy violations in OSNs on economic well-being is closely related to what has been discussed so far. Privacy-friendliness can function as a seal of quality of OSNs and may increase their value which has been shown by Tsai et al. (2007)[242] and Böhme and Koble (2007)[243]. Therefore, privacy threats to OSNs may diminish their value.

---

237 Wisniewski et al. 2012.
238 See Goffman 1973. See also Deleuze/Guattari 1987. And see Whitehead 1941.
239 Miller reports of an informant (Marvin), whose marriage got into trouble. After having fought with his wife in the networked public of Facebook, there is no chance of forgetting about the issue. Miller 2011, p. 12.
240 boyd 2007.
241 Wang et al. 2011.
242 boyd 2007, p. 9.
243 Tsai et al. 2007.

5.4 THREATS TO PRIVACY IN E-COMMERCE AND THEIR CONSEQUENCES FOR THE CORE VALUES

As there is a close connection between OSNs and e-commerce, much of what has been said about threats to privacy in OSNs and their consequences for the core values also applies to e-commerce scenarios. However, while users typically deal with only a few OSN providers, in the e-commerce scenario, many more actors are involved, for example search engines for locating goods and best offers, online merchants, and banks. This makes the threats to privacy even more serious.

As for OSNs, also in the e-commerce context, adequate levels of user awareness, user control, and trustworthiness of the e-commerce platforms ensure privacy protection. Awareness again refers to the users understanding the relevant aspects of the policies regarding personal user data applied by the numerous e-commerce participants. Personal data that is directly submitted by e-commerce users is, for example, payment information, comments on products, and wish lists. Personal information that is generated by data processing includes browsing habits, interests, and shopping behaviour. Awareness also refers to e-commerce platforms being sufficiently trustworthy to respect regulations and user preferences. Control again refers to the users being able to influence the policies in such a way that their privacy preferences are respected, e.g. in regard to sharing their data with third parties. Finally, the condition trustworthiness refers to all e-commerce actors' responsibility to respect user preferences, the relevant privacy laws, and to provide appropriate data protection.

As in OSNs, awareness, control, and trustworthiness for e-commerce platforms are not yet satisfactory. User awareness is threatened as the many e-commerce actors require and collect differing amounts of personal data, and use it for many purposes, for example targeted advertising, and analysing user behaviour and preferences.[244] Also, user awareness is challenged as the e-commerce actors apply (different) privacy policies that may not be available or comprehensible for the users.[245, 246] Also user control is threatened in e-commerce as the control mechanisms provided by the many e-commerce participants may be unsatisfactory or unusable. Finally, trustworthiness of e-commerce platforms is threatened. Local laws and regulations may be inappropriate for the digital world. Given the global character of e-commerce it is unclear which law is applicable. Also, in view of the large number of participating institutions it appears to be extremely challenging to establish convincing auditing mechanisms. Finally, implementing appropriate data protection mechanisms is very challenging and costly, particularly for small enterprises that participate in e-commerce.[247, 248] As for OSNs, a lack of awareness, control, and trustworthiness may lead to serious threats to privacy: decontextualization, re-purposing, tracking, re-identification, and data persistence.

The threats to e-commerce privacy challenge the core values of free self-determination, democratic participation, and economic well-being. The analogous discussion for OSNs is also applicable here. In addition, there are a few more issues specific to e-commerce. As buying goods and services on the Internet is becoming inevitable, users are forced to accept the privacy standards of the e-commerce vendors. For example, users may be deprived of the possibility of refusing to be tracked and profiled and receiving targeted offers, although these practices are not a primary purpose of the interaction between customers and online vendors (re-purposing and decontextualization)[249]. This leads to users not obtaining equal treatment, e.g. lowest offers and

244 Böhme et al 2007.
245 Suggesting that this effect is widely unwanted: Turow et al. 2009, pp. 1-27.
246 Roßnagel et al. 2003, p. 184.
247 Nissenbaum 2011, p. 35; Turow et al.2005, p. 26.
248 PWC 2011.
249 Recent data breach incidents are proof of that, e.g., yahoo data leak from July 13, 2012 (TAZ.de 2012) but also with the Amazon daughter Zappos.com, Inc. in early 2012 (Financial Times Deutschland 2012) as well as Sony in 2011 (Süddeutsche 2011).

pricing.[250, 251, 252] The multitude of channels (e.g. email, vendor web sites, OSNs) and methods[253] (e.g. demographics of the customer, analysis of past buying behaviour, user comments and ratings, tracking and re-identification) make this a very serious threat to self-determination. The same mechanisms may also have a negative effect on democratic participation. E-commerce profiles of political candidates could be used against them by their competitors. Profile-based targeted advertising may also be used in the context of political elections. Finally, these techniques may also have a negative impact on economic well-being. Customers may not get the best offers and prices and vendors may obtain unfair advantages over their competitors.

5.5 CONCLUSION

We have shown in this chapter how privacy may be compromised in online social networks and that these privacy violations may have a negative impact on the three core values of free self-determination, democratic participation, and economic well-being. In order to reduce the negative impact on the core values, it is important to satisfy the basic privacy conditions of awareness, control, and trustworthiness laid out in Section 5.1 as much as possible. Options on how to fulfil said conditions by implementing the appropriate measures are presented in Chapter 6 of this document.

250 Schaumann 2013 gives the example of a 17-year-old searching for weight loss products and solutions who is presented with weight loss ads which make her focus on that topic and thus reinforcing that "interest" in a negative way.
251 Turow et al. 2005, p. 25.
252 Singer 2011.
253 Spiekermann 2006, pp. 47-52.

6 OPTIONS FOR ACHIEVING PRIVACY IN ONLINE SOCIAL NETWORKS AND E-COMMERCE

In Chapter 4 we have explained how OSNs can support the core values identified in Chapter 2: democratic participation, free self-determination, and economic well-being. In Chapter 5 we have identified, firstly, conditions that, when met, enable the implementation of these values: awareness, control, and trustworthiness. In a second step, we have identified a set of threats to the implementation of these values, and shown how they relate to the conditions: decontextualization, persistence, and re-identification. In this chapter, we present possible scopes of action, or *options*, that can help enable the conditions and counter the threats.

Both OSNs and e-commerce are terms that go well beyond their technical implementations. While OSNs encompass their usage and the societal consequences of this usage, e-commerce also refers to the economic, and therefore societal, institution to enable e-commerce as another form of commerce. This broader societal perspective motivates our decision to provide options for achieving privacy and trust in one combined chapter.

This societal perspective also intuitively explains why OSNs and e-commerce share many commonalities when it comes to a culture of privacy and trust on the Internet, as defined by the core values and conditions identified in Chapter 5. The number of players may be different; their roles might differ slightly; and the amount of data may be different: regardless of all these variations, we do not see a qualitative difference. The options for OSNs transcend the application domain of OSNs (and OSN technology will continue to be a likely technical option for e-commerce as well). It is also noteworthy that recommendation infrastructures for e-commerce can be seen as social networks in themselves. The oft-quoted difference that in e-commerce privacy is part of the product characteristics[254], for instance, the material a product is made of does not change this observation of the fundamental congruence of the two domains of OSNs and e-commerce. Offering and choosing among privacy policies, and screening or controlling their enforcement is identical for both OSN and e-commerce. Options to achieve privacy and trust are valid for both. From an economic perspective, the major difference is that in e-commerce, real products are exchanged and the seller expects compensation; from the perspective of a culture of privacy and trust, this difference appears to be immaterial.

In general, implementing anonymity and using pseudonyms comes as an exception to this rule: the exchange of goods and compensations typically requires knowing the identity of the respective other party. However, when taking into account that the electronic advertisement industry is part of every e-commerce marketplace (and this is the most obvious connection between OSNs and e-commerce), anonymity and pseudonymity intuitively are desired tools from a customer's perspective as far as the advertisement-related actors are involved. The other participants in an e-commerce marketplace tend to have a natural interest in privacy: In OSNs, data is made (semi-)public, while in e-commerce this usually is considered an upfront violation of trust.

As a consequence of these considerations, this chapter contains a common description of options for both OSNs and e-commerce. To avoid abstraction, we deliberately formulate the options primarily in terms of OSNs, nevertheless, every single option directly applies to e-commerce as well. Distinctive idiosyncrasies of the e-commerce domain will be highlighted as such.

We group the scopes of action, or options mentioned in the first paragraph, into three sets that complement each other: technology, education, and formal regulations/rules/good practices. The need to combine the different classes of approaches – technological, regulatory, and educational – is exemplified as follows. The derived privacy conditions can be enabled by *technology*. For example, cryptography-based authentication technologies help protect personal user data from unauthorized access. However, OSN users may not trust that OSN providers properly deploy such technology. Such trust can be established by a *legal* regulation that requires

254 Schafer et al. 1999, pp. 158, 160, 161.

the use of advanced authentication technology and a corresponding auditing process that establishes the compliance of the OSN provider's processes and technologies with the regulation. However, technology and regulations are not sufficient. For instance, if OSN services are designed in a way that modern smart-card based authentication technology is required, average OSN users may not know how to use it appropriately. Thus, user *education* is necessary. Finally, not all privacy risks can be prevented by technology, regulations and consumer education. As in the non-cyber world, *good practices* support privacy in areas not covered by regulations. For example, it is a good practice that people do not abuse private information which they have been granted access to.

In the following paragraphs, we present options for technology, regulations, education and good practices that enable awareness, control, and trustworthiness in OSNs and e-commerce and, at the same time, counter the abstract threats of decontextualization, persistence, and re-identification. The goal is to impair the positive effects of OSNs and e-commerce on the core values as little as possible. However, we defer an analysis of the respective trade-offs to the final recommendations provided by the project. In this spirit, we do not provide recommendations with regard to any of these options: every option has advantages and shortcomings, and the assessment is often non-trivial. As an example, the benefits of a regulatory duty by the OSN to inform users about the dissemination of personal data are unclear if this means that twenty such messages pertaining to a single user are sent every day, or if the recipient cannot be expected to understand what this means. In this document, we do not take into account practicality or feasibility considerations.

Not providing recommendations and trade-off analysis in this document also means that we deliberately do not provide careful analysis of the options, but rather merely present them as such.

The remainder of this section is organised as follows. For each of the enabling conditions of awareness, control, and trustworthiness, we discuss options in terms of regulations, technology, and education (awareness: Section 6.1; control: Section 6.2; trustworthiness: Section 6.3). We indicate for each option which threat it potentially combats, i.e., decontextualization, persistence and re-identification. With the relationship between threats and core values already laid out in Section 4, we only occasionally refer to the directly impacted core values. Section 6.4 concludes.

6.1 AWARENESS

6.1.1 REGULATORY OPTIONS FOR AWARENESS

In terms of awareness, there is one fundamental regulatory option:

OSN providers' duty to inform

User awareness in regard to OSNs refers to users' ability to know and understand how and which aspects of their personal data is available to whom on an OSN, for what purpose, and how that data is processed and disseminated. Acting self-determinately requires awareness of the modes and results of processing personal data. To provide the respective transparency, privacy policies would need to address specific information about the structure and methods of data processing, about how individual pieces of data are being used, for what purpose; and to whom it is accessible. Privacy policies would then need to be accessible at all times and be updated instantly with regard to the data processing policies adopted by social network providers.[255] To this end, transparency regulations would need to establish the duty to provide information in a clear and understandable format[256], this specifically includes a reasonable decision about aggregations and omissions. It might be helpful to

255 Following the common perspective that every characteristic of a production and distribution process is part of the product, and that a buyer also decides on these characteristics.

256 Roßnagel et al. 2001, p. 86.

develop standard privacy policies by legislation[257] or – if appropriate – by means of self-regulation.[258] Privacy settings would need to be specific and differentiated to simultaneously offer a variety of possibilities and be understandable and usable.

European and German data protection regulations already contain provisions concerning information that needs to be disclosed to the user. That information includes the identity of the responsible person with regard to data collection, processing and storage, the purpose of data retention, to whom the data is accessible, as well as rights the user has against the responsible person (e.g. Art. 10, 11 DPD[259], §§ 5, 13 TMG, § 4.3 BDSG). Future regulations could also include information related to the structure and methods of data processing and the respective physical systems, as well as to the handling of derived data, in order to make data retention more transparent. In addition, future data protection regimes may require that the information given be provided in a clear and understandable language for the average user (similar to the current legal regulations concerning consumer law, § 307.1.2 BGB[260]). This must also be seen in connection with the principle of informed consent.

In terms of e-commerce, every (market) regulation tends to aim at protecting the buyers and, as a consequence, to restrict the sellers. The "E-Commerce-Directive" contains requirements for "information society services"[261] concerning transparency in e-marketing and e-communication and for the liability of service providers. Therefore, the "E-Commerce-Directive" has been implemented in Germany by the Telemediengesetz. The EU directive might be taken as a model to overcome the location principle of regulation.

6.1.2 TECHNICAL OPTIONS

There are two major ways that awareness can be enabled by technology: transparency-enhancing technologies (TETs) and notification tools.

Transparency-enhancing technologies

One technical option to enhance privacy awareness is for providers of social network services to deploy, and for users to embrace, transparency-enhancing technologies (TETs). There are two classes of TETs that can be leveraged to identify, assess, and mitigate risks related to the lack of awareness on OSNs: *user-side tools* and *provider-side tools*. Usually designed as visualization tools and browser extensions, user-side TETs are pieces of technology that help notify users, or anyone acting on their behalf, about the intended collection, storage, processing, and/or further sharing of their personal data, including inferences drawn from that data, for instance, interest profiles on the grounds of surfing behaviour in the OSN. In addition, user-side TETs typically provide capabilities that may assist OSN users in understanding how much sensitive information they have (intentionally or unintentionally) disclosed, the disclosure contexts, as well as what privacy consequences/risks this might bear (i.e. their levels of privacy). It is also conceivable that such TETs provide estimates, in euros, of how valuable the data they are providing to the OSN actually is. This would also be applicable to user profiles that aggregate several sources. User-side tools include, among other techniques, icons and labels for non-verbal privacy notices[262], machine-readable formats and related agents (nudges) for signalling and negotiating privacy policies, and privacy dashboards deployed on the users' end. In contrast, provider-side TETs are tools that are deployed in the OSN operator's back-end system. They provide OSN users access to their stored

257 Roßnagel et al. 2011, p. 169. The EU-Commission Draft for a General Data Protection Regulation would establish this duty in Art. 11.2.
258 Bundestag 2011, p. 54.
259 Roßnagel et al. 2001, p. 154.
260 EU Data Protection Directive 95/49/EC.
261 German Civil Code – Bürgerliches Gesetzbuch.
262 Art. 1.2 of the EU Directive 98/34/EC as amended by the EU directive 98/48/EC: "'service', any Information Society service, that is to say, any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services."

personal data as well as information on how it has been processed. Users can make use of these kind of TETs, firstly to view and monitor how and for which purposes their data has been processed, secondly to opt-out of certain uses of their personal information or certain services, and thirdly to inform themselves as to whether all this is in compliance with existing privacy standards and/or policies negotiated with the provider. By defining and allowing users access to appropriate APIs, provider-side TETs can give consumers, possibly via apps, access to their OSN (possibly derived) data. This allows opportunities to assess the impact of participating in OSNs on their lives. Another dimension in which today's dashboards, in particular the provider-specific dashboards, exhibit room for development is that they concentrate on data managed by a single provider. The concept of "federated" dashboards is one option to tackle this challenge. By interfacing with different OSN sites, providing details about what personal data was shared, with whom, in which OSN, and for what purpose, federated dashboards would support the OSN users in understanding the full picture of their online social networking identity. Such federated dashboards can be viewed as an integration point for various tools that, among other things, may assist OSN users in exercises their right to informational self-determination.

In terms of e-commerce, user-side TETs may not necessarily seem to be useful tools when it comes to the mere end-to-end exchange of goods against money. From the customers' perspective, however, user-side TETs might turn out to be useful, when considering that shopping and browsing data is collected by intermediaries such as general brokers. It is worth noting that while brokers may collect this data in order to provide and improve their services, they may not necessarily have an interest in sharing this data, or only to a limited extent, because it is this data on which their business is built. Moreover, provider-side TETs appear to be necessary technology when the customers' right to be informed (§34.1 BDSG) is enforced – upon request, responsible parties have to convey which data is stored for a customer, its provenance, and potential parties to whom the data was forwarded, and the purpose. Generalized TETs for intra- and inter-business data tracking are then necessary – but also lead to a fundamental contradiction between the data protection goals of transparency and avoided aggregation of personal data ("Nicht-Verknüpfbarkeit"). Usage control technology might be a technical option for tracking data provenance; resolving the aforementioned fundamental conflict is a societal and legal challenge.

Notification tools

A second option to enable transparency in Internet-based social networking is to deploy notification tools. These tools would automatically let OSN users know that privacy breaches have occurred on the provider's side. More importantly, they would help both the provider and the users to understand possible implications of such breaches. In spite of the rather straightforward notification features currently supported by some OSN sites, an implementation of a meaningful notification strategy (i.e., one that would additionally give insights into possible implications of a privacy breach) does not seem to have been implemented by any platform yet. A possible reason for this is the potential negative influence of such a strategy on the OSN's performance and the provider's image.

There does not seem to be a difference between these kinds of notification tools for OSNs and e-commerce.

6.1.3 EDUCATIONAL OPTIONS

Internet-related socio-technical structures are shaped by a multitude of actors, including users, providers, educators etc. Generating awareness therefore pertains to all the relevant actors involved. In what follows we will identify these actors; sketch relevant content to be communicated to them; and specify the methods for doing so.

Relevant actors

Although the overwhelming majority of OSN users are young people, this is not the only group to be targeted. All those who frequently interact with youth are a relevant target group (thereby acting as a kind of multiplier) as well as those who create the socio-technical structures within which the action takes place. While educators sometimes lack a sufficient understanding of the workings and difficulties coming with frequent OSN use,[263] they are only able to assist young users if they are knowledgeable in these matters. We have identified the following groups:[264] students at school, students at university, apprentices, parents, educators/teaching staff at regular and professional schools, journalists, and providers' staff.

While the first three groups are the ones to be targeted directly, parents and teaching staff might assist them. Journalists are addressed here as multipliers. However, given the press coverage the privacy issue has gotten in recent years, there does not seem to be too much need for action as far as they are concerned. The providers' staff certainly has a lot of influence on the shape of socio-technical structures and is therefore a relevant target for creating awareness.

Content of awareness raising activities

A first field of action could be to develop a widespread understanding of, broadly speaking, the *individual* as well as the *collective* challenges that might come with privacy violations on OSNs: traces left unwittingly in OSNs (see Chapter 5.2.1), the sensitivity of personal information fed deliberately into OSNs, the fact that any utterance on OSNs is at least visible to the provider and thus never as private as an offline conversation, the risk of compromising other users' privacy by feeding information about them into OSNs (e.g., images showing friends), and the question of whether or not OSNs are trustworthy, and what that means. In sum, there are three dimensions to be addressed: technology, economic aspects, and rights and duties.

Understanding of preferences and the OSN

Assessing the privacy policies of a particular OSN and examining the extent to which these policies match individual preferences presupposes two intellectual capabilities: first, a reflection on one's own preferences; and second, at least a rough understanding of the workings of OSNs and of the technological possibilities of OSN providers to process and capitalize on data. This includes quality and quantity of explicitly provided and implicitly collected data, the visibility of data for other users, providers, and third parties, and the processing, disclosure, modification and terms of storage (see Section 5.1.1). For example, users only have the chance to realistically assess the privacy policies of a third party app provider if they are aware of 1) what kind of information they (don't) want to disclose to whom, and 2) what can be done with their information by the OSN as well as the app provider, including the possibility of recombination of previously separated data items (decontextualization, re-identification). When informed about what information a certain app extracts from a user's profile (e.g. on Facebook: "This App Needs: Your profile info... Your Stories... Friends' profile Info... Stories shared with you...") it appears possible to make an informed decision if there is awareness of the providers' technical possibilities to work with the users' information, such as tracking users across different web domains (see Chapter 5.2.3), and the generation of new information via inferences (Chapter 5.2.2).

Understanding of the business's interests

Many users do not have a clear understanding of the providers' business models and interests, and thus of the value of the provided data.[265] Consequently, they have a rough

263 Such privacy notices would provide a snapshot of the provider's privacy policy, making it more comprehensible for users.

264 Kammerl/ 2010, Livingstone et al. 2011.

265 The listing is based on the German Bundestag's Enquete-Kommission "Internet und digitale Gesellschaft", Projektgruppe Medienkompetenz account (Bundestag 2011, pp. 20-31). We have selected those groups that are relevant as regards OSN usage and also added a few groups that are not mentioned in the report.

idea of providers working with personal information, but they may not have in mind that gaining and analysing such information forms the core of their business model. Thus, users' attention could be directed to the fact that they are dealing with businesses in the first place, and that their activities are therefore part of some economic value chain. Without awareness of the economic aspects of OSN procedures, it seems impossible to fully understand the implications of certain specifications and expressions contained in the providers' terms of service.

Understanding of rights and duties

This is particularly important when it comes to OSN privacy policies, because many users lack a clear understanding of, and/or feel unable to cope with the legal situation on the Internet. Thus, they either think of the Internet as some kind of space where the law can only be enforced in a limited way; or they falsely assume themselves to be protected by legal regulations when in fact they are not.[266] Some users are not necessarily interested in their rights simply because they do not care. Users must be aware of the sensitivity of data retention policies, and they must learn methods to call in the compliance of providers, and where to turn to in case of infringement[267]. Providers could be made aware of the sensitivity of the information they handle every day, so as to make them take more responsibility.

Awareness training methods

Depending on the particular target group and content, there are several possible awareness training methods.

Broadcasting and viral campaigns

In order to raise the general public's awareness of OSN-related privacy issues, a valuable strategy could be to stage advertising campaigns via broadcasting networks and the like. Responsible authorities could develop spots for broadcast on TV and in movie theatres as well as posters and ads in magazines.[268] As far as parents are concerned, it might prove difficult to reach this group; presentations given at schools and other public places could

---

266 Turow et al. 2005, for instance, found in a 2005 telephone survey that "most Americans who use the Internet have little idea how vulnerable they are to abuse by online and offline marketers and how the information they provide can be used to exploit them (...)" The study's findings suggest a complex mix of ignorance and knowledge, fear and bravado, realism and idealism that leaves most Internet-using adult American shoppers open to financial exploitation by retailers." (ibid.: p. 3) This "mix of ignorance and knowledge" was mirrored in our own focus group study by participants indicating that, while they have a rough idea of the providers being somehow interested in their data, they do not know exactly what providers can do with their data; they doubt it is at all possible for providers to analyse all the data divulged; and, anyway they do not feed sensitive data into OSNs, which is why there would be no point for providers to be interested in it. In this sense, there is a misconception in many users' perspectives that perfectly fits the findings of a follow-up study of Turow et al. 2009, where the authors state, "In fact, our survey found that Americans want openness with marketers. If marketers want to continue to use various forms of behavioural targeting in their interactions with Americans, they must work with policymakers to open up the process so that individuals can learn exactly how their information is being collected and used, and then exercise control over their data." Turow et al.2009, p. 5.

267 Evidence is again provided by the sources already quoted in the previous footnote. One quote from our own focus group study is exemplary for users' assumptions of the law only being enforceable in a limited way on the Internet: „Diese Sache mit dem Studenten, der sich da die Daten hat zuschicken lassen, da hat er ja dann irgendwie auch, soweit ich es mitbekommen habe, festgestellt, dass da gewisse Dinge fehlen, gewisse Einträge oder Nachrichten. Und hat dann noch mal sich mit Facebook in Verbindung gesetzt und gefragt, wo denn der Rest ist, ein gewisser prozentualer Anteil, der fehlt, wo Facebook daraufhin meinte, „nee, das ist Unseres, das geben wir nicht raus, das ist jetzt geheim". Also quasi das gesamte Recht über deine Daten, die du da abgetreten hast. Es ist einfach so unüberschaubar. Und deswegen würde ich auch komplett damit übereinstimmen, wenn man sagt, man hat keine Kontrolle darüber, man *kann* das gar nicht wissen, was mit den ganzen Sachen passiert." Turow et al. confirms for the American case: „The survey further reveals that the majority of adults who use the Internet do not know where to turn for help if their personal information is used illegally online or offline." (Turow et al. 2005, p. 3); at the same time, however, "Americans mistakenly believe that current government laws restrict companies from selling wide-ranging data about them. When asked true-false questions about companies' rights to share and sell information about their activities online and off, respondents on average answer only 1.5 of 5 online laws and 1.7 of the 4 offline laws correctly because they falsely assume government regulations prohibit the sale of data." (Turow et al. 2009, p. 4) Thus, whether under- or overestimating the rule of law on the Internet, many users have an incorrect conception of the legal situation on the Internet.

268 It is also possible to develop seals of quality for OSNs indicating the compliance of a given provider; as far as these are concerned, the educational task would be to make users aware of the existence and relevance of those seals in order to measure the trustworthiness of various OSN providers.

nevertheless provide them with the information required. An option to address the target group of young people would be to induce viral campaigns, which means to systematically spread the message to the users where they are, i.e., in OSNs themselves.[269]

Systematic education at school and beyond

As far as teaching staff and educators are concerned, it is common that the skills of students exceed those of the teachers. Some researchers therefore call for a special training for educators of all kinds.[270] Honing in on those making the heaviest use of OSNs, i.e. young people, suggests that a promising place to develop an understanding of the privacy issues related to OSNs is school. Thus, it may be conceivable to introduce a new school subject, similar to German language teaching or mathematics. In this case, the technical intricacies of OSNs could be made a component of media literacy classes,[271] taught by specialised teachers. An alternative would be to weave Internet privacy through the overall curriculum, with all of the teachers and educators receiving training on this topic. Still another option would be to develop Internet safety training in a similar model to drivers' education courses. Given the extraordinary pace of innovation on the Internet, however, one also might consider tackling the issue by providing schools with space, time, and infrastructure for students to learn from their peers. Developing detailed training programs takes significant time, therefore they might already be outdated by the time they are implemented. From this perspective, then, self-organised learning processes of the students, with the teachers acting as navigators or catalysts of the educational process[272] could turn out to be a viable option.

Educational options in terms of e-commerce seem less numerous – in an explicit e-commerce setting, the customers already know that the business partner pursues business interests. Gaining an understanding of which data is collected while engaging in e-commerce, and how this data can be (ab)used, is a general skill that can be taught in similar fashion to the options for OSNs.

6.2 CONTROL

6.2.1 CONTROL BY REGULATION

Once privacy preferences have been established, users need to be able to formulate them and initiate their implementation in order to be able to control the collection, processing and storage of their personal data.

Isolated, explicit consent

From the perspective of regulations and informal rules, one option is to make user consent explicit and isolate it rather than integrate it in general provisions (as already stipulated by regulations). Users could be asked to repeatedly re-provide or withdraw their consent at regular intervals in case they change their mind about the use of their data.[273] For the purpose of clarity, consent for data processing could be disconnected from the terms of service by having separate options (buttons) to give consent or withdraw it at any time. Furthermore, opt-in concerning data processing can be made a general default. This would also raise user awareness concerning their rights because they would actively have to make decisions regarding the

269 To give an example, Federal Government Crime prevention has developed a cartoon pointing out the dangers of feeding images of third parties into OSNs. The material can be ordered free of charge by teachers and distributed freely within schools. Krempl 2012.

270 Bundestag 2011, p. 34.

271 Kammerl 2010, p. 57.

272 In this respect, the level of awareness within media pedagogy expert circles could be improved. For example, the Enquete-Kommission "Internet und digitale Gesellschaft" mentions privacy in those documents dealing with media literacy and education only rarely (Bundestag 2011). It is therefore not too surprising that the Konferenz der Datenschutzbeauftragten des Bundes und der Länder recently published an Entschließung titled „Datenschutz als Bildungsaufgabe", calling for data protection to be included as a basic element of media literacy education (Konferenz der Datenschutzbeauftragten des Bundes und der Länder 2011, p. 159).

273 Bundestag 2011, p. 23.

policies. If desired, in order to nudge users to utilise their privacy preferences and corresponding software agents to manage their online privacy, OSN providers could be committed to the standardisation of interfaces and information for their platforms.[274]

In terms of e-commerce, similar options apply. It is worth repeating that there is a difference between explicitly provided data – data that, among other things, pertains to shipping addresses, bank accounts, or product IDs – and implicitly provided data such as browsing behaviour or correlations with other data sets.

Anonymization, pseudonyms

Control with respect to choice/consent includes the right to use services anonymously or under pseudonym. In this way, the user may limit the amount of personal data disclosed to the OSN provider. A pseudonym is a fake name which is used instead of the real name to hide the true identity. This concept is already implemented in current German legislation. However, said legislation is limited to the anonymization of data only when it is no longer needed, or as long as it is technically possible and reasonable (as is the case in § 13.6 TMG). Some OSN providers argue that a pseudonymous usage is not possible.[275] This objection notwithstanding, the right to anonymous or pseudonymous usage could be established as a general binding rule.[276] Because an OSN provider or third parties in limited cases may have the need to know the real name of a user in specific situations, one option is to give users the chance to provide their real name and additionally choose a nickname which would be the one made public. The real name could be provided to third parties who act as trustees or intermediates.

In terms of e-commerce, anonymization and pseudonymization need to be implemented in a way that business can still be executed – money must be transferred, and goods need to be shipped. In contrast, these techniques can be applied to (derivations of) data and secondary data (e.g., browsing) along the chain of intermediaries, as long as business can still be executed.

Communication of users' rights and withdrawal of consent

To further enable informational self-determination, exercising user rights might be made easier, for example, when they do not approve of how their data is used, or if they change their mind about sharing certain information on an OSN. As discussed in Section 6.1.1 above, raising awareness includes providing certain information about users' rights in an understandable and clear form. It seems reasonable to assume that only then will users be able to exercise their rights regarding control of their data. Legal regulation could state that the execution of rights should be possible electronically, allowing execution to be unimpeded and free of charge, and avoiding cross-media conversion.[277] Since an OSN user in many cases cannot know who receives personal information, withdrawal of consent could commit the recipient of the consent and the withdrawal to forward the withdrawal to all known recipients.[278] Also, the initial withdrawal could legally bind all further recipients; also with reference to inferred or processed data.

In terms of e-commerce, this option does not seem to apply to the data strictly necessary to conduct business, but does seem applicable to other (derived) data.

---

274 Roßnagel 2007, p. 179; Roßnagel et al.2001, p. 70.
275 Roßnagel 2007, p. 179.
276 Facebook 2012: Facebook cannot plausibly explain why it does not allow pseudonymous usage with unreasonableness or impossibility, only that its goal is to have real people connect on the platform.
277 Roßnagel et al. 2001, p. 148.
278 Roßnagel et al. 2001, p. 169.

National borders

General provisions might consider applicable national data protection regulations which may not be determined by the location of the OSN server but rather by the location of the user.[279] In this way, users would always be able to know which regulations apply to the processing of their personal information. Thus, they could decide whether they want to proceed, based on the knowledge of what information may be legitimately processed and what rights they would possess. However, the problem of enforcement of the applicable (national) law if the OSN provider has registered the office outside of the jurisdiction remains.The same considerations apply to e-commerce.

Correction, blocking, deletion

Control over one's data includes the possibility to delete this data. Some legal regulations oblige providers to delete user data upon request (instead of hiding it from view and storing it anyway). Clear technical definitions of "deletion" are required. Users could be entitled to automatically receive a confirmation that data was deleted successfully.[280] It should be noted, however, that the deletion obligation would be limited to the sphere of the OSN or the service provider but would not ensure a successful deletion of data in the World Wide Web.

Current regulations do provide certain rights for users, especially in regard to correction, blocking, or deletion, e.g., Art. 12 DPD or § 35 BDSG. Especially on the Internet, however and here especially in OSNs, it is hard to enforce these rights if the provider does not comply with current legislation. Imposed sanctions could raise the willingness to comply with current data protection standards, as could incentives like certificates for providers which could be used as marketing tools. Both will be explained below.The same considerations apply to e-commerce.

Expiration

In order to implement data minimisation and user control, it is possible from a regulatory perspective to dictate expiration dates for personal data, including photos.[281] The same considerations apply to e-commerce.

6.2.2 TECHNICAL OPTIONS FOR CONTROL

In this section, we address OSN-specific technologies only. As service providers, OSN providers can of course deploy additional, non-OSN specific, server-side mechanisms (e.g. provenance tracking, usage control) that would help enforce privacy requirements.

Privacy-friendly default configurations and settings

The first technical option for improved user control in OSNs is to provide privacy settings for user profiles that provide a high degree of privacy by default. Privacy settings would need to be intuitive, making it even easier for average users to set their preferences regarding the handling (how, when – expiration dates – and by whom) of their personal data or to make changes that would reflect their privacy preferences and needs. In order to achieve this goal, if they do not already do so, OSN service providers may want to consider usability from the outset as one of their functional requirements (privacy-by-design).[282] This implies involving users (or research participants) and their feedback in the engineering process of their privacy-setting models. One possible area of improvement for privacy settings within user profiles is to design them in a way that would make the user's prior consent a requirement for tagging that person in a photo or a video (which already is implemented in several OSNs). Furthermore, profile privacy settings are to be designed in a way that would allow user control not only over direct but also over downstream use of their data, e.g., possibly inferred

279 Enquete-Kommission 2012: Fünfter Zwischenbericht der Enquete-Kommission 2012, p. 54.
280 European Commission 2012: The EU-Commission Draft for a General Data Protection Regulation would follow this approach in Art. 3.2.
281 Roßnagel et al. 2001, p. 177.
282 Enquete-Kommission 2012, p. 55.

or aggregated data that may be shared with advertisers. User preference models could be designed in a way that the customer or trusted entities are able to verify that the preferences were not bypassed. In addition, user preference models could enable messaging controls, i.e., ensuring that only friends can send and receive messages (that comply with their preferences) between each other. This is also already partially implemented by some OSNs.

The same considerations apply to e-commerce. Once more, the distinction between data strictly necessary to conduct business between customer and seller and relevant intermediaries, and data that is not strictly necessary is relevant here: Default privacy settings seem particularly relevant for the latter because they are usually implicitly collected.

Note that an implementation of this option in OSNs would give users effective control over their reputation and their digital self-representation. Indeed, providing the OSN users with specific, detailed choices about the processing (collection, use and sharing) of personal data would enable them to regulate information about themselves on the OSN, support informed and selective disclosure of intimate details, and allow them to counter and correct misinformation.

Leverage transparency tools

The second option to achieve customer empowerment is to leverage existing transparency and awareness tools and technologies and build OSN-specific privacy feedback and awareness (PFA) solutions. PFA tools can be based on the TET tools discussed above (remember that these help increase OSN users' awareness of the kinds of information they have shared or are about to share as well as the possible privacy implications). In addition, and more specifically, they would provide more possibilities for users' control by allowing them to react to the information they are provided: seeing what is happening does not always automatically mean one knows how to react to this information.

The same APIs as discussed in the context of TETs for awareness could also be used to empower OSN users to rectify and/or delete pieces of their personal data held by the OSN provider. A prominent example of a provider-side dashboard is the Google Dashboard[283]. It allows Google service users to access a summary of data associated with their Google Accounts. In order to move beyond the current state and address some of the limitations of existing TETs[284, 285] there still seems to be room for improvement in terms of usability Current dashboards do not consider the handling of derived data (e.g., the "strength" of links between people as measured by the number of messages exchanged in-between them).

Further examples of control exercised by users include hiding their data, i.e. by not uploading it, encrypting it, setting restrictive profile privacy setting rules, or deleting it from OSN provider servers. When deployed on the user side, PFA would put the users in control and help them prevent inadvertent disclosure of private data. They could provide real-time reminders, e.g. in the form of short on-screen messages, indicating that the information the user is about to share can be potentially sensitive personal data and that this may carry some privacy risks down the road. The underlying concept here is the notion of "privacy nudges"[286, 287] with the acknowledged risk of patronising users. By leveraging machine learning techniques and models from the field of behavioural economics, such solutions could nudge users participating in online networking activities in ways that they would consider beneficial for the protection of their privacy.

The same considerations apply to e-commerce, particularly so for data that is not strictly necessary to execute the business at hand.

283 European Commission 2012.
284 Google 2012.
285 Ghiglieri et al. 2012.
286 Waidner et al. 2011, pp. 1-20.
287 Acquisti 2009, pp. 82-85.

Data minimisation

A third option to enhance user control in OSNs is to provide them with the means to regulate the amount of personal information they release when registering for, accessing, consuming or terminating an online social networking service. This can be achieved by implementing and using 1) data minimisation technologies, 2) privacy-dedicated credential and identity management models that take group and individuals' levels of trust into account and allow (dynamic) policy negotiation, and 3) decentralized architecture models for computing and data management. Data minimisation, for instance, may include offering users the option to create and use revocable anonymous profiles, and/or browser extensions that would help to prevent unauthorized access to OSN users' content by encrypting those files before uploading or sharing them on the OSN platform. On the other hand, an implementation of identity management (IdM) models and standards in an OSN ecosystem would allow OSN users to (jointly) manage both the context-dependent disclosure of certain personal data and the accessibility to that information, e.g. to make selected identity information visible only to a selected audience. This way, IdM may help users to define and enforce their audience and context segregation policies on OSNs.[288, 289, 290] Moreover, such an integration of user-centric identity management concepts into OSNs may create a situation where OSN service providers could easily accommodate users' privacy preferences, and thus be able to work with minimal personal data. However, researchers have pointed out that current identity and access control systems may need to be readjusted when applied to OSNs[291, 292]. In an attempt to improve that situation, privacy researchers have proposed privacy mechanisms (e.g. Lipford's Privacy Mirror[293] and LeFevre's Privacy Wizard[294]) that extend the set of features already provided by existing social network platforms and/or design entirely new OSN architecture supporting identity management (e.g. Primelife Clique[295], PCO[296]). The concepts that have been proposed to help users manage their audiences, contacts, and other personal information is very similar to the Google+ circles which are meant to mimic the offline social practice of audience segregation, online. Another aspect of this option is to let OSN users have control over downstream use of certain pieces of their data, e.g., by setting and enforcing purpose constraints for third party application providers. Concepts and technologies that can support this aspect include opting out of online behavioural tracking via Opt-out Cookies, Do Not Track options built into web browsers and usage control frameworks[297, 298, 299].

These considerations should be viewed in the context of Web 2.0 where interactions with an OSN do not necessarily happen on the OSN provider's side (e.g., +1 or like buttons).

The same considerations apply to e-commerce, particularly so for data that is not strictly necessary to execute business.

Portability

The fourth technical option for increased user control in the context of OSNs is to provide users with means to exercise their right to data portability. To free users from

288 Kelley et al. 2010, pp. 1573-1582.
289 van den Berg 2010, pp. 1111-1116.
290 Rahman et al. 2010, pp. 41-48.
291 Lipford et al. 2008.
292 Madejski et al. 2011.
293 Weiss 2008, pp. 161-171.
294 Lipford et al. 2008.
295 Fang/LeFevre 2010, pp. 351-360.
296 van den Berg 2010, pp. 1111-1116.
297 Rahman et al. 2010, pp. 41-48.
298 Kumari et al. 2011, pp. 85-96.
299 Lovat/Pretschner 2011, pp. 151-152.

de facto lock-ins and to thus enable informational self-determination, OSN sites could implement and provide free access to application programming interfaces that can enable OSN users to transfer their (profile) data between different social network platforms while simultaneously maintaining privacy protection. In order to prevent a situation where one single OSN provider would be able to diminish the autonomy and personal choice of users, any meaningful tool for supporting users' right to data portability would have to rely on open standards and interoperable IT technologies. The current draft of the EU Commission General Data Protection Regulation also adopts the right to data portability in Art. 18.2 a. This option does not seem to apply to e-commerce.

A related control option that applies to e-commerce, is a technical implementation of the "right to be forgotten." This privacy right is a centrepiece of the European data protection framework proposed in 2011. The notion of "right to be forgotten" aims at addressing privacy-related threats emerging in digital ecosystems (which OSNs are examples thereof) due to data persistence. Indeed, data persistence makes it hard for OSN users to interact with each other (e.g. express controversial thoughts) , without the threat of being unable to escape their past since easily reproducible details of these interactions may continue to live "forever" somewhere in the cloud. Hence a meaningful option is to provide OSN user with simple, easy to use yet effective tools for permanent and complete account deletion. Recently[300], ENISA overviewed the state of existing techniques for expiration of data.[301] Unfortunately, none of these techniques provide strong guarantees with regard to an enforcement of the right to be forgotten in scenarios such as OSNs and e-commerce. ENISA points out the fact that the right to be forgotten cannot be ensured solely by relying on technology, and also highlighted a number of research gaps.

6.2.3 EDUCATIONAL MEASURES REGARDING CONTROL

Educational measures that address the understanding of an OSN's structures, concepts, policies, rights, and obligations have been discussed in terms of educational measures regarding awareness. Such knowledge about what is happening needs to be complemented by knowledge about how to possibly change the course of action. This kind of media literacy can be seen as a further cornerstone. Again, we will proceed by specifying relevant target groups, contents, and methods.

Relevant actor

Educational measures geared toward increasing the level of user control have a natural focus on users themselves, those teaching them, and those shaping the interactive structures in question:[302] students at school, students attending university, apprentices, teaching staff/educators at regular and professional schools, providers' staff (first and third party, e.g. app providers).

Note that the first three groups are the actual target, with the fourth group serving a multiplier function, and the fifth participating in the development of privacy-friendly practices on the providers' side.

Content of control increasing activity

Controlling the flow of information in OSNs appears possible only when considering diverse components: norms, policies, and skills.

Informational norms duties

As privacy is an inherently social, i.e., collective phenomenon, the social groups using OSNs need to be aware of the fact that they can only maintain the privacy of all the group's members as well as that of the group as a whole if

300 Pretschner et al. 2011, pp. 122-140.
301 Kalabis 2012, pp. 670-675.
302 Druschel et al. 2011.

they agree to negotiate informational norms that are binding for everyone. For instance, to protect the privacy of all the users concerned, a peer group might specify that photos may only be uploaded after consulting all the people being shown in the picture. Once the norm is established, it is possible to demand that others adhere to it: social control may be executed in ways that sanction specific practices. On the providers' side, norms may contribute to the development of best practice standards within the industry. As they gain more and more relevance, engaging clients, such as third party app providers, in awareness-raising activities also is an option.

Understanding and formulating policies

In order to make privacy policies beneficial to the users, the latter may need to be able to use the technical features implementing those policies to full capacity. This would require an increase in user skills: 1) users need to have a clear understanding of their own privacy preferences, 2) of the way those preferences are affected by the technical workings of OSNs, and 3) of the technical features that are suitable to shape the flow of information in a way that matches their privacy preferences. In other words, users need to have the necessary competencies to translate privacy preferences into privacy settings and practices, *vis-à-vis* other users as well as providers and third parties.

Developing & increasing skills

In order to stay in control as much as possible, one needs to comprehend the – often difficult to understand and hard to use (see 5.2.2) – privacy settings of particular OSNs. At the core are questions like: what kind of information becomes accessible to which party (other users, provider, third parties) under what conditions? How to control the visibility of the personal information fed into the network: how to give/cancel consent for collection, processing, disclosure of data for app providers (or other third parties)? How to move, modify, and delete (if possible) data? How to determine the visibility of data to whom, and for how long? How to segregate different audiences? How to determine retention time? As re-identification and tracking technologies have the potential to violate privacy preferences (see 5.1.2 and 5.2.2), the distribution of techniques fending off tracking and guaranteeing anonymity might also be desirable. In this regard, easy-to-use applications and add-ons, such as Tor[303], Ghostery[304], or Mozilla's Better Privacy[305] could be included in training content. This way, users' room to maneuver could be enlarged, for awareness and skills once acquired are likely to remain and to be put to new contexts by users.[306]

Control training methods

There are three ways to increase control on the users' side via education: training in school, self-education, or with providers' support.

Training in school

Again, there are several options how to configure teaching in school (new required subject, collective self-education, etc.). As they have been already discussed above, we will not elaborate on that at this point.

Self educating tutorials

An alternative to the dissemination of skills at school would be to develop self-education tools, privacy tutorials, technical means (demonstrations, videos) and the like, tailored to specific user groups. However, the usage of such tools would require extra effort by the users, the only incentive being a current absence of potential damage in the future. While an appropriate solution for individually-motivated users, others would have to be "nudged" to concern themselves with these tools. In other words, a soft paternalism strategy that encompasses "nudging

303 Enquete-Kommission 2012, pp. 20-31. We restrict the listing to those groups that are empirically the heaviest users of OSNs (thus, we do not include pre-school children and seniors, who might make use of the Internet, but who are usually not very active on OSNs).
304 Tor 2013.
305 Ghostery 2012.
306 Mozilla 2012.

privacy"[307] could turn out to be a viable option to make users successfully complete privacy tutorials (e.g., making it mandatory to complete a privacy tutorial before granting users permission to register in an OSN; we omit discussing the ethical implications such paternalism raises).

Educating providers' staff

As stated above, the providers can play a role in strengthening user control; this might be achieved by developing and implementing norms guiding providers' staff behaviour. Such norms might be translated into formalized terms of service, for instance, by being formulated in a consolidated, clear and understandable way. To this end, systematic education of OSNs' staff and management, as well as the development and promotion of (internally) good privacy practices in workplace could be desirable. This could be acquired by accomplishing privacy-awareness training presentations, providing videos, FAQs about privacy policies and practices, etc.

The same considerations apply to e-commerce, particularly so for data that is not strictly necessary to execute the business.

6.3 TRUSTWORTHINESS

While awareness, transparency and control are essential for improving privacy in OSNs, it is also necessary to improve users' trust of each other (establishment and management of trustworthy user relationships within OSNs) as well as the trustworthiness of the OSN providers' data processing practices.

6.3.1 TRUSTWORTHINESS BY REGULATION AND RULES

Trustworthiness of providers in relation to data processing, disclosure, purpose and context binding, safety of data and data minimisation could be regulated via two different approaches. The first one would impose duties on OSN providers, and the second one would promote trustworthiness by rewarding good conduct and behaviour. Also, general provisions could be considered in order to create a homogeneous set of rules.

Stricter fines, consequences

To further increase awareness among providers concerning the importance of different privacy principles and encourage providers to comply with privacy regulations, stricter fines, penalties and other consequences could be imposed. Those general principles would protect personal data, avoid data retention where possible and include the principles of purpose, necessity and data avoidance or minimisation. They therefore address our conditions and threats. They are already codified in European and German regulations. However, their breach is rarely directly connected to any consequences for the responsible entity. Specifically, the principles of data minimisation and avoidance are not connected to any rules of infringement and therefore raise no consequences in case of a breach.[308]

Breaking up monopolies

In the case that monopolies are identified, the resulting and underlying lock-in has the immediate potential to lead to all privacy threats discussed in this document. One option is to forbid and dissolve such monopolies.

Competitors' complaints

To enforce higher-level privacy standards between businesses one could consider competitors' complaints so that data breaches would be considered unfair competition or abuse of market position. Providers would be encouraged to fulfil privacy regulations or face consequential lawsuits and, possibly, fines.[309] Private institutions could enforce omissions of unfair competition and begin legal actions when necessary. This is, in fact, codified in specific consumer protection

[307] boyd/Hargittai 2010.
[308] Acquisti 2009, pp. 82-85.
[309] Hornung 2011, p. 53.

regulations already, and could be extended to data protection regulations in general.[310]

Specifications

Guidelines and specifications could be issued by data protection authorities.[311] Regulations about terms and conditions of service are generally consumer-friendly. However, there is still room for improvement. To ensure a high level of privacy, terms of service could be tightened to leave manufacturers (who design the services or technical means to use them) and providers little or no margin to deviate from consumer-friendly regulations.

Protection of minors

To raise the level of trust regarding the protection of minors, age verification systems and systems for parental consent could become obligatory where minors are expected to have access to the service.[312] Legal regulation in this respect appears extensive and cohesive. However, it still lacks technical implementation in online services.

Intangible damages and strict liability

The tort system for data protection breaches by private entities could be expanded to encompass intangible damages, e.g. emotional distress after severe violation of one's right to privacy[313]. Also, the liability regime could be transformed into a strict liability in tort.[314] This kind of a tort system would empower users to achieve compensation for damages effectively, and thus possibly discourage breaches on the part of the providers. Providers would be liable for any breach of data protection regulation without proof of responsibility, unless they can sufficiently prove that they have fulfilled every rule that they were obligated to by law.

Escalation

Acknowledging that the innovation curve in the Internet is steep and that services are often developed in close collaboration with the user, differences arising around the proper handling of data and compliance with the rules and privacy regimes may be escalated to mediation or alternative dispute resolution bodies.

Strengthening independent authorities

The organisation and standing of independent (privacy) authorities could be strengthened. Independent data protection authorities are one way to maintain a high level of privacy standards and are established in current regulations. Furthermore, the different functional responsibilities of public data protection authorities, e.g., private/public and federal/state as well as state/state, may turn out to be more effective if coordinated centrally. They could be granted more extensive rights, especially the right to give binding instructions based on the law.[315] Private data protection authorities' powers and responsibilities could also be strengthened and their independence from their inspection body could be enforced. That is especially important where they may be impeded from consulting higher authorities out of fear of repression, thus it is important to improve their contractual rights and protect them from termination of their employment.[316]

Basic points for privacy by design

Privacy by design aims at integrating data protection standards into services and products from the start, above all by high-standard privacy settings by default. Basic points for Privacy by design might be laid down in legal specifications, for example: which general privacy principles could

310 Roßnagel et al. 2001, p. 203.
311 Roßnagel et al. 2001, p. 204.
312 The EU-Commission Draft for a General Data Protection Regulation contains numerous delegated acts which empower the Commission to adopt non-legislative acts of general application to supplement or amend certain non-essential elements of a legislative act (quasi-legislative acts).
313 The EU-Commission Draft for a General Data Protection Regulation would establish comparable approaches in Art. 8.1.2.
314 Roßnagel et al. 2001, p. 182.
315 Roßnagel 2007, p. 196.
316 Roßnagel et al. 2001, pp. 189,195.

and should be furthered by services and technology and who should be held to implement such technical privacy standards (manufacturers/service providers). Concrete solutions for these basic points might, however better be left to technical developers.

Audits, certificates, privacy seals

Audit processes and certificates could enable users to assess the privacy-friendliness of their OSN of choice. This would of course also require awareness of the certification processes itself, the baselines against which certification takes place, and of the respective guarantees from the users' perspective. In order to make it easier for users and providers to assess the quality of certificates, different national or European initiatives could be integrated under one brand.[317]

It seems possible to make the use of privacy and security seals by OSN providers mandatory (but the following treatise is independent of whether these seals are required or used as marketing tools, similar to the seals of German "Stiftung Warentest"). The key idea behind these privacy seals is that IT-based services' compliance with privacy standards and data protection regulations can be certified and reliably signaled to consumers, which, however, does not allow for relevant end-user consequences such as "my data will never be lost". The certification as well as the issuing of seals is ideally performed by an independent organisation. The respective privacy requirements and standards typically oblige providers to disclose information about what personal data they collect, how and for what purpose that data will be processed and/or further shared, and possible control options the user has. This way, privacy seals could help increase transparency with regard to how data controllers (i.e. website operators) handle personal information and subsequently enhance users' trust and confidence on the Internet. When visiting a website that has been certified, i.e. that displays a privacy seal, and based on the details the provider discloses, users should be able to make informed decisions about whether or not to reveal their personal data to the website (even though this possibly would require the provisioning of end-user guarantees of the abovementioned kind, which is usually not the case). In the context of OSNs, privacy seals could be used to send clear signals to the (prospective) users, indicating that the OSN provider adheres to certain security and privacy standards, e.g. ISO 27001, and that users' data would be collected and processed accordingly. Facebook and Google+ are both licensees of the commercial TRUSTe Privacy Program[318]. However, other privacy and security seals issued by programs such as EuroPriSe (European Privacy Seal[319]), BBBOnLine[320] or WebTrust[321] are rarely used in the context of OSNs, at least not by popular social networking sites. In Germany there already exists a privacy seal provided by the data protection authority of the German state Schleswig-Holstein[322], and there is the currently planned "Stiftung Datenschutz". The unification of this multiplicity of seals is another option to improve privacy in OSNs, also considering that services are often provided worldwide, the relevance of a European or German seal is limited.

Self-regulation

Self-regulation aims at committing companies, providers etc. to complying with self-imposed rules. In order to establish binding and reliable rules of data protection, basic ground rules by the legislator could provide the opportunity to be concretised and extended by joint agreements between companies and consumer associations. Among other things, self-regulation could be applied to defining the necessity of collecting different data for different

317 Roßnagel et al. 2001, p. 198.
318 Enquete-Kommission 2012, p. 54.
319 TRUSTe 2013.
320 Europrise 2013.
321 Better Business Bureau 2013.
322 Trust Services 2013.

purposes; to procedures of realizing anonymization and pseudonymization; to trade-specific rules of informing users about data retention procedures and necessary rules of safety measures; and expiration dates for personal data. Incentives may be necessary to for the development of self-regulations. To guarantee that self-regulations are reviewed in regular intervals and still provide sufficient protection for personal data, an expiration date could be established.[323]

International regulation

Cross-border issues, especially which law is applicable and where and how to enforce users' rights, can be addressed by either self-regulation or international binding legislation. Although unification is taking place today, a worldwide data protection law is not yet in sight, and on an international level, self-regulation alone is not likely to be sufficient.

A first step in international legislation has been taken within the European Union. The Data Protection Directive 95/46/EC has been amended several times and provides ground rules concerning data retention for each member state to be transposed into national law, but at the same time leaving the national legislator room to maneuver, and to establish more detailed and stricter rules. The new Draft of General Data Protection Regulation[324] will provide binding rules for each member state without the need or possibility for transposition. While the specific realisation of that regulation has been widely and controversially discussed,[325] the idea of establishing a general rule for all European countries – by way of directive or regulation – naturally is one option.

All these considerations also apply to e-commerce.

6.3.2 TECHNICAL OPTIONS REGARDING TRUSTWORTHINESS

Trustworthy OSN ecosystems rely on (1) trust between one OSN user and another (2) trust between users and providers.

Cooperative behaviour, User-Centric/Community-Centric Identity Management

This can be achieved by deploying technologies that promote cooperative behaviour checking and by effective controls and identity management. For example, these technologies used in conjunction with information from the social graph could help OSN users to assess the level of trust within their communities, so as to figure out if a friendship request is trustworthy or more generally to decide whom they should trust when entering new virtual friendships or consuming third party online social networking services. By leveraging feedback and recommendations by other users (friends and contacts), cooperative behaviour checking tools would provide OSN users with means to judge a stranger with whom they are about to establish a relationship, and quantitatively assess potential risks, in terms of unintended disclosure of private information, of befriending that stranger.

Trust but verify: Trustworthiness of OSN provider

A second option to enhance trustworthiness in OSNs is to allow users to assess the trustworthiness being offered by the OSN provider and enable automatic verification of provider compliance with both privacy regulatory requirements and users' data handling preferences. This approach could help address some of the limitations of current "static" certification methodologies that relate to the structure of organisations and their IT[326] information security. Existing

323 Independent Centre for Privacy Protection Schleswig-Holstein 2013.
324 Roßnagel et al. 2001, p. 153.
325 Proposed by the European Commission 2012.
326 The current scholarly and political discussion shows that while the regulation brings about some improvement, on the whole there are many issues that need to be re-evaluated: Hornung 2012, p. 99; Masing 2012, p. 2305; Nebel/Richter 2012, p. 407; Eckhardt 2012, p. 195; Roßnagel 2012, p. 553; Masing 2012, p. 9 (and many more). Regarding the hearing in the German Bundestag on 22 October 2012: Krempl 2012.

certification methodologies may be proved insufficient when applied to OSN systems that meld various kinds of services, hosted in dynamic environments. An implementation of automated security assurance and compliance tools would provide not only individual users but also organisations with compliance responsibilities and data protection authorities the ability to remotely and quickly confirm whether the OSN provider's platform and back-end system are secure (to an extent to be defined) and that the obligations with regard to the handling of personal data are being carried out. Technical options here include data provenance tracking and trustworthy logging tools for audits. It needs to be taken into account that if usage of data is tracked, this may lead to second-level privacy issues: the new data creates new privacy challenges.

All these considerations also apply to e-commerce.

6.3.3 EDUCATIONAL MEASURES REGARDING TRUSTWORTHINESS

Generating trustworthiness is primarily a matter of legislation and technology (establishing a widely accepted seal is not a user's core business), with educational measures being mainly associated with the acknowledgment of trust-creating mechanisms.

Relevant actors

In this respect, educational measures pertain primarily to two target groups: users and providers.

While users need to be made aware of mechanisms, such as seals, and are also required to be able to honor the effort providers make in order to create trust, providers are bound to take measures that make them deserve trust.

Content of Activities Increasing Trustworthiness

Trustworthiness can be improved if users are empowered to detect and understand if their privacy preferences are indeed respected by a given provider. This requires three areas of practical knowledge

1. How to monitor the information fed into the network (e.g. how to download a copy of the divulged data)

2. How to use some OSN internal features or some standalone software tool allowing to check whether the privacy settings do indeed match the privacy preferences

3. Understanding of certification processes that is sufficient to assess which user guarantees are effectively provided

In addition, users are likely to need knowledge of the crucial issues concerning trustworthiness (see Section 5.1.3) such as collecting, processing, disclosing regulations; purpose and context binding; data minimisation; anonymization; and OSN security. Providers' staff could be required to be trained in trust building activities.

Trust Building Training Methods

It is possible to create the capability of users to realistically assess the trustworthiness of individual OSNs via training in schools, universities and tutorials. However, increasing trust in OSN providers could be achieved by establishing trustworthiness standards and training providers' staff accordingly.

All these considerations also apply to e-commerce.

6.4. CONCLUSION

In Chapter 5, we have abstractly argued how the implementation of the core values of informational self-determination, democratic participation and economic well-being can (1) be enabled by the three conditions of awareness, control,

and trustworthiness and (2) be impeded by the threats of decontextualization, persistence, and re-identification.

In this chapter, we concretised these considerations by providing options for action in terms of regulations and rules, technology, and education. We are convinced that a culture of privacy and trust relies on a combination of approaches from these domains.

We have formulated the options mainly in terms of OSNs. This is because the options largely overlap, as spelled out in the introductory remarks of this section. Where applicable, we have indicated relevant differences. A major distinction is made between data that is strictly necessary to execute a business transaction (product ID, bank account, shipping address) and every other (derived) data, e.g., browsing behaviour on broker platforms, clicks on ads, etc. We would like to re-emphasize that recommendation platforms for e-commerce provide hints at a convergence of these two technologies.

In terms of regulations, we identified only a few options that are bound to awareness where OSN providers (or e-commerce actors) could be encouraged to unveil specific parts of their inner workings, including their approaches to processing and dissemination of (possibly derived) data, while at the same time making sure that this unveiled data can be understood and processed by the recipients. This is because the respective regulatory body is already rather comprehensive – but as of yet arguably lacks enforcement. In terms of *control*, however, regulations could mainly require privacy-friendly default settings and dashboards through which deletion requests, for instance, could be issued. As far as *trustworthiness* is concerned, privacy seals open up an entire range of options, where user- friendliness could be improved by avoiding the existence of innumerable seals.

In terms of technology, *awareness* can be increased by several existing transparency enhancing tools, including dashboards. We have made a distinction between server-side and client-side mechanisms, where the former seem particularly relevant when data provenance is to be provided upon inquiry. These technical options can – and today sometimes are – also be used for issuing privacy-related commands to an OSN (or e-commerce platform). Verification that the displayed data corresponds to reality and that the issued commands are actually executed needs to be enforced by further means and is the subject of technology for complementary auditing approaches to trustworthiness. Note again that also in these parts of the document, we have deliberately restricted ourselves to technology that is directly concerned with OSNs (trustworthy logging capabilities by providers, for instance, transcend the domain of OSNs and, specifically, also apply to e-commerce).

In terms of education, roughly understanding (1) privacy concepts, abstract and concrete risks as well as consequences of providing data, preferences, and the technology behind OSNs (and Web 2.0 and e-commerce players), stakeholder motivations and (2) understanding the medium of OSNs and the navigation in OSNs (in e-commerce) is bound to awareness. This includes the communication between users and the OSN as well as the communication between one OSN user and another. Media competence in terms of understanding what privacy policy settings actually mean (and what they do not mean) provides means for *control*. As far as *trustworthiness* is concerned, a basic understanding of certification for law or privacy seals and the actualisation of provided guarantees seems bound to establish trust in the context of OSNs.

We have indicated how each of these options potentially addresses one of the three threats identified in Chapter 5.

We have deliberately not provided any recommendations in this chapter. There are multiple trade-offs between practicality, usability, economic feasibility, etc. that need to be addressed before such recommendations can be provided. This is the subject of the acatech POSITION[327].

[327] acatech 2013.

LITERATURE

Aberjhani 2012
Aberjhani: *Catching up with Our Humanity*. 2012. URL: http://www.guerrilla-decontextualization.net/1/category/all/1.html [as of: 11/08/2012].

acatech 2013
acatech (Ed.): *Privatheit im Internet. Chancen wahrnehmen, Risiken einschätzen, Vertrauen gestalten* (acatech POSITION), Heidelberg et al.: Springer Verlag 2013.

Acquisti 2009
Acquisti, A.: *Nudging Privacy: The Behavioural Economics of Personal Information*, 2009. URL: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5370707&isnumber=5370689 [as of: 18.02.2013].

Akerlof 1970
Akerlof, G.: The Market for "Lemons". In: *Quarterly Journal of Economics*, 1970. URL: http://www.project-syndicate.org/commentary/asymmetries-of-information-and-economic-policy/german [as of: 08.02.2013].

Altman 1975
Altman, I.: *The Environment and Social Behavior*, Monterey, CA.: Brooks/Cole 1975.

Anderson 2006
Anderson, C.: *The Long Tail. Why the Future of Business is Selling Less of More*, New York, NY: Hyperion 2006.

Augusto 2007
Augusto, J.: *Ambient intelligence: the confluence of ubiquitous/pervasive computing and artificial intelligence, Intelligent Computing Everywhere*, London: Springer Verlag 2007.

Bakos 1997
Bakos, J.: "Reducing buyer search costs: Implications for electronic marketplaces". In: *Management Science*, Vol. 43, 1997, pp. 1676-1692.

Bauman 2009
Bauman, Z.: *Leben als Konsum*, Hamburg: Hamburger Edition 2009.

Benkel 2012
Benkel, T.: "Die Strategie der Sichtbarmachung. Zur Selbstdarstellungslogik bei Facebook". In: *Kommunikation@Gesellschaft*, Jg. 13, Beitrag 3, 2012. URL: http://www.ssoar.info/ssoar/bitstream/handle/document/28270/B3_2012_Benkel.pdf [as of: 26.02.2013].

Better Business Bureau 2013 a
Better Business Bureau: *Assurance on the Internet*, 2013. URL: http://www.bbb.org/us/bbb-online-business/ [as of: 18.02.2013].

Better Business Bureau 2013 b
Better Business Bureau: *What Complaints do we handle? How do we handle your complaints?*, 2013. URL.: www.bbb.org/complaints/aboutResolution [as of: 25.02.2013].

Beye et al. 2012
Beye, M./Jeckmans, A./Erkin, Z./Hartel, P./Lagendijk, R./Tang, Q. "Privacy in Online Social Networks". In: *Computational Social Networks: Security and Privacy*. London: Springer Verlag 2012, pp. 87-113.

BILD.de 2012
BILD.de: *Horror-Bilanz einer Facebook-Party*, 2012. URL: http://www.bild.de/news/inland/facebook-party/mehrere-verletzte-26106558.bild.html [as of: 09/09/2012].

BITKOM 2011
BITKOM: *Soziale Netzwerke. Eine repräsentative Untersuchung zur Nutzung sozialer Netzwerke im Internet*, 2011. URL: http://www.bitkom.org/files/documents/BITKOM_Publikation_Soziale_Netzwerke.pdf [as of: 14.01.2012].

Böhme/Koble/Dresden 2007
Böhme, R./Koble, S./Dresden, T.: *On the viability of privacy-enhancing technologies in a self-regulated business-to consumer market: Will privacy remain a luxury good?*, Workshop on the Economics of Information Security (WEIS), Carnegie Mellon University, Pittsburgh, PA 2007.

Bonneau/Anderson/Danezis 2009
Bonneau, J./Anderson, J./Danezis, G.: *Prying Data out of a Social Network, Proceedings of the 2009 International Conference on Advances in Social Network Analysis and Mining* (ASONAM '09), IEEE Computer Society, Washington, DC 2009.

Bonneau et al. 2009
Bonneau, J./Anderson, J./Stajano, F./Anderson, R.: *Eight Friends are Enough: Social Graph Approximation via Public Listings, Proceedings of the Second ACM EuroSys Workshop on Social Network Systems* (SNS '09), ACM, New York, NY 2009.

Borchers 2012
Borchers, D.: "Das Netz vergisst nichts" (Aufklärungscomic vorgestellt), 2012. URL: http://www.heise.de/newsticker/meldung/Aufklaerungscomic-Das-Netz-vergisst-nichts-vorgestellt-1662075.html [as of: 25.10.12].

Bourdieu 1982
Bourdieu, P.: *Die feinen Unterschiede. Kritik der gesellschaftlichen Urteilskraft*, Suhrkamp, Frankfurt am Main 1982.

boyd 2007
boyd, d.: *Why Youth (Heart) Social Network Sites: The Role of Networked Publics in Teenage Social Life*, 2007. URL: http://www.danah.org/papers/WhyYouthHeart.pdf [as of: 08.02.2013].

boyd/Ellison 2007
boyd, d./Ellison, N.: *Social Network Sites: Definition, History, and Scholarship - Journal of Computer-Mediated Communication*, 2007. URL: http://jcmc.indiana.edu/vol13/issue1/boyd.ellison.html [as of: 08.02.2013].

boyd 2008
boyd, d.: "Facebook's Privacy Trainwreck: Exposure, Invasion, and Social Convergence." In: *Convergence. The International Journal of Research into New Media Technologies*, 14, Nr. 1, 2008, pp. 13–20.

boyd/Hargittai 2010
boyd, d./Hargittai, E.: "Facebook Privacy Settings: Who Cares?" In: *First Monday*, Volume 15, Number 8 - 2 August 2010. URL: http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/3086 [as of: 18.02.2013].

Brynjolfsson et al. 2011
Brynjolfsson, E./Hitt, L./Kim, H.: *Strength in Numbers: How Does Data-Driven Decisionmaking Affect Firm Performance?* 2011. URL: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1819486 [as of: 15.03.2013].

Brynjolfsson/Saunders 2009
Brynjolfsson, E./Saunders, A.: *Wired for Innovation: How Information Technology is Reshaping the Economy*, Cambridge, MA: MIT Press 2009.

Brynjolfsson/Saunders 2010
Brynjolfsson, E./Saunders, A.: *Wired for innovation: how information technology is reshaping the economy*, Cambridge, MA: MIT Press 2010.

Buchmann 2012
Buchmann, J. (Ed.): *Internet Privacy – Eine multidisziplinäre Bestandsaufnahme/A multidisciplinary analysis* (acatech STUDIE), Heidelberg et al.: Springer Verlag 2012.

Bundestag 2011
German Bundestag's Enquete-Kommission "Internet und digitale Gesellschaft", Projektgruppe Medienkompetenz account, 2011. URL: http://www.bundestag.de/internetenquete/dokumentation/Medienkompetenz/Zwischenbericht_Medienkompetenz_1707286.pdf and Handlungsempfehlungen URL: http://www.bundestag.de/internetenquete/dokumentation/Sitzungen/20120625/A-Drs_17_24_052_-_PG_Bildung_und_Forschung_Handlungsempfehlungen.pdf [as of: 25.10.12].

Callon 1998
Callon, M.: "An essay on framing and overflowing: economic externalities revisited by sociology" and Introduction: The embededness of economic markets in economics". In: Callon, M. (ed.): *The Laws of the Markets*, Oxford: Wiley-Blackwell 1998.

Callon 1986
Callon, M.: "Some Elements of a Sociology of Translation: Domestication of the Scallops and the Fishermen of St. Brieuc Bay". In: John Law (Hg.): *Power, Action, and Belief: A New Sociology of Knowledge?*, London: Routledge & Kegan Paul 1986, pp. 196–233.

CBC News Montreal 2009
CBC News Montreal: *Depressed Woman Loses Benefits Over Facebook Photos*, 2009. URL: http://www.cbc.ca/news/canada/montreal/story/2009/11/19/quebec-facebook-sick-leave-benefits.html [as of: 18.02.2013].

Chakrabarty 2007
Chakrabarty, D.: *Provincializing Europe: Postcolonial Thought and Historical Difference*, Princeton, NJ: Princeton University Press 2007.

Cheng 2012
Cheng, J.: *Over 3 years later, "deleted" Facebook photos are still online*. 2012 URL: http://arstechnica.com/business/2012/02/nearly-3-years-later-deleted-facebook-photos-are-still-online/ [as of: 18.02.2013].

Compliance Week 2011
Compliance Week: *ISACA Issues New Social Media Audit Program*, URL: http://www.complianceweek.com/isaca-issues-new-social-media-audit-program/article/197773/ [as of: 07.03.2011].

Deleuze/Guattari 1987
Deleuze, G./Guattari, F.: *A Thousand Plateaus: Capitalism and Schizophrenia, Minneapolis*, MN: University of Minnesota Press 1987.

Deloitte 2012 a
Deloitte: *Internal Audit (IA) for Social Media- Discussion Document*, 2012 URL: http://www.isaca.org/Education/Upcoming-Events/Documents/ISACA-Social-Media-Assessment-Discussion-Document.pdf [as of: 26/06/2012].

Deloitte 2012 b
Deloitte: *Measuring Facebook's Impact in Europe, Executive Summary*, 2012 URL: http://www.deloitte.com/assets/Dcom-UnitedKingdom/Local%20Assets/Documents/Industries/TMT/uk-tmt-media-facebook-europe-economic-impact-exec-summary.pdf [as of: 26/06/2012].

Deutschland Funk 2011
Deutschland Funk: *Ägypten ist keine „Twitter Revolution"*. 2011. URL: http://dradio.de/dlf/sendungen/interview_dlf/1382263/ [as of: 02.05.2012].

DIVSI 2012
Deutsches Institut für Vertrauen und Sicherheit im Internet (DIVSI): *DIVSI Milieu-Studie zu Vertrauen und Sicherheit im Internet*, 2012. URL: https://www.divsi.de/sites/default/files/presse/docs/DIVSI-Milieu-Studie_Gesamtfassung.pdf [01.03.2012].

Draft for a Data Protection Regulation 2012
Draft for a Data Protection Regulation in Europe by the EU-Commission COM (2012) 11 from 25th January 2012. URL: http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0010:FIN:EN:PDF [19/02/2012].

Dreier 2006
Dreier, H.: *Grundgesetz, Kommentar*, Band II (2. Auflage), Tübingen 2006, Art.20 GG (Demokratie), Rn. 83.

Druschel et al. 2011
Druschel, P./Backes, M./Tirtea, R./Tirtea, R./Ikonomou, D.: "The right to be forgotten – between expectations and practice". In: *Enisa Report 2011*. URL: http://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/the-right-to-be-forgotten/at_download/fullReport [as of: 18.10.2011].

Dumortier 2009
Dumortier, F.: "Facebook and Risks of 'De-contextualization' of Information". In: Gutwirth, S./Poullet, Y./ De Hert, P.: *Data Protection in a Profiled World*, Heidelberg: Springer Netherlands 2009.

Eckhardt 2012
Echardt, J.: "EU-DatenschutzVO – Ein Schreckgespenst oder Fortschritt?". In: *Computer und Recht* (CR) 3/2012, pp. 195-203.

EGE 2012
EGE Opinion No. 26 "Ethics of Information and Communication Technologies", 2012 URL: http://ec.europa.eu/bepa/european-group-ethics/docs/publications/ict_final_22_february-adopted.pdf [as of: 04.03.2013].

Ellison 2007
Ellison, N./Steinfield, C./Lampe, C.: "The Benefits of Facebook ''Friends'': Social Capital and College Students' Use of Online Social Network Sites". In: *Journal of Computer-Mediated Communication*, Vol. 12, 2007. URL: http://jcmc.indiana.edu/vol12/issue4/ellison.html [as of: 19.02.2013].

Ellison/Steinfield/Lampe 2007
Ellison, N./Steinfield, C./Lampe, C.: "The Benefits of Facebook ''Friends'': Social Capital and College Students' Use of Online Social Network Sites". In: *Journal of Computer-Mediated Communication*, 12(4), article 1. URL: http://jcmc.indiana.edu/vol12/issue4/ellison.html [as of: 08.02.2013].

Enquete-Kommission 2012
Fünfter Zwischenbericht der Enquete-Kommission „Internet und digitale Gesellschaft": Datenschutz, Persönlichkeitsrechte, Bundestags-Drucksache 17/8999, 15.3.2012, 54. URL: http://www.bundestag.de/internetenquete/dokumentation/Zwischenberichte/Zwischenbericht_Datenschutz_1708999.pdf [as of: 19.02.2013].

European Commission 2012
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), 2012. URL: http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf [as of: 19.02.2013].

EU Directive 95/46/EC
EU 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 of the EC, 23, 1995, L 281.

EU Directive 95/49/EC
Data Protection Directive 95/49/EC of the European Parliament and of the Council on the capital adequacy of investment firms and credit institutions. Official Journal of the EC, 1995, L 177.

EU Directive 98/34/EC
EU Directive 98/34/EC of the European Parliament and of the Council on a procedure for the provision of information in the field of technical standards and regulations and of rules on Information Society Services, Official Journal of the EC, 1998, L 204.

EU Directive 00/31/EC
EU Directive 00/31/EC of the European Parliament and of the Council on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce), Official Journal of the EC, 2000, L 178/1.

EU Directive 00/78/EC
EU Directive 00/78/EC establishing a general framework for equal treatment in employment and occupation, 27 November 2000, Official Journal 2000, L 303, 16-22.

EU Directive 01/29/EC
EU Directive 01/29/EC of the European Parliament and of the Council on the harmonisation of certain aspects of copyright and related rights in the information society, Official Journal of the EC 2001, L 167.

EU Directive 02/58/EC
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), Official Journal of the EC 2002, L 201, p. 37-47.

EU Directive 06/24/EC
EU Directive 06/24/EC of the European Parliament and of the Council on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, Official Journal of the EC 2006, L 105.

EU Directive 06/54/EC
EU Directive 06/54/EC of the European Parliament and of the Council on the implementation of the principle of equal opportunities and equal treatment of men and women in matters of employment and occupation (recast), 5 July 2006, Official Journal 2006, L 180, 22-26.

EU Directive 09/58/EC
EU Directive 09/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector, 12 July 2002, Official Journal 2002, L 201 p. 37-47; amended by the Directive 2009/136/EC (Cookie Directive), 25 November 2009, Official Journal 2009, L 337, 11-36, which has not yet been implemented into German law.

Europe versus Facebook 2012 a
Europe versus Facebook, 2012. URL: http://www.europe-v-facebook.org/DE/Anzeigen/anzeigen.html [as of: 19.02.2013].

Europe versus Facebook 2012 b
Europe versus Facebook, 2012. URL: http://www.europe-v-facebook.org/removed_content.pdf [as of: 19.02.2013].

Europrise 2013
Europrise European Privacy Seal, 2013. URL: https://www.european-privacy-seal.eu/ [as of: 19.02.2013].

Facebook 2011
Facebook Inc.: *Data Use Policy*, 2011. URL: http://www.facebook.com/full_data_use_policy [as of: 19.02.2013].

Facebook 2012
Facebook Inc.: *Full Data Use Policy*, 2012. URL: https://www.facebook.com/full_data_use_policy [as of: 19.02.2013].

Facebook 2013 a
Facebook Inc.: *Facebook for Websites*, 2013. URL: http://developers.facebook.com/docs/guides/web/ [as of: 19.02.2013].

Facebook 2013 b
Facebook Inc.: *People You May Know*, 2013. URL: http://www.facebook.com/help/501283333222485/ [19.02.2013].

Fang/LeFevre 2010
Fang, L./LeFevre, K.: "Privacy wizards for social networking sites". In: *Proceedings of the19th International Conference on World Wide Web, WWW '10*, New York, NY: ACM, 2010, pp. 351-360.

Farrell/Klemperer 2007
Farrell, J./Klemperer, P.: "Coordination and lock-in: Competition with switching costs and network effects". In: Armstrong, M./ Porter, R.: *Handbook of Industrial Organisation*, London/Amsterdam/New York, NY: Elsevier, 2007, 3, pp. 1967-2072.

FTC 1998
Federal Trade Commission: *Privacy Online: A Report to Congress*, 1998. URL: http://www.ftc.gov/reports/privacy3/priv-23a.pdf [as of: 19.02.2013].

FTC 2012
Federal Trade Commission: *Protecting America's Consumers*, 2012. URL: http://www.ftc.gov/reports/privacy3/fairinfo.shtm [as of: 04.03.2013].

FTC v. Toysmart.com, LLC 2000
Federal Trade Commission v. Toysmart.com, LLC, 2000 WL 34016434 (US District Court, District of Massachusetts, July 21, 2000)

Financial Times Deutschland 2012
Financial Times Deutschland: *Datenklau bei Amazon-Schuhladen Zappos*, 2012. URL: https://www.ftd.de/it-medien/medien-Internet/:hackerangriff-datenklau-bei-amazon-schuhladen-zappos/60155343.html [as of: 25.02.2013].

Fluglärm Mainz 2012
Fluglärm Mainz – Initiative gegen Fluglärm Mainz Oberstadt, 2012. URL: http://www.facebook.com/pages/Fluglaerm-Mainz-Initiative-gegen-Flugl%C3%A4rm-Mainz-Oberstadt/150873958350995 [02.05.2012].

Fowler 2012
Fowler, G.: "When the Most Personal Secrets Get Outed on Facebook". In: *The Wall Street Journal*, 2012. URL: http://online.wsj.com/article/SB10000872396390444165804578008740578200224.html [as of: 26.02.2013].

Frankfurt Nord 2012
Frankfurt Nord gegen Fluglärm, 2012. URL: (http://frankfurt-nord-gegen-fluglaerm.de/) [as of: 02.05.2012].

FÜR Stuttgart 21 2012
FÜR Stuttgart 21, 2012. URL: (http://de-de.facebook.com/fuer.s21) [as of: 02.05.2012].

Future of Advertising 2011
Future of Advertising 2015 (Studie), 2011. URL: http://medien.nrw.de/wp-content/uploads/2011/09/2011_Studie_Future_of_Advertising.pdf [as of: 01.03.2013].

General Assembly 2000
Resolution adopted by the General Assembly [without reference to a Main Committee (A/55/L.2)] 55/2, 2000.URL: http://www.un.org/millennium/declaration/ares552e.htm. [as of: 25.02.2013].

Ghiglieri/Simo/Waidner 2012
Ghiglieri, M./Hervais, S./Waidner, M.: *Technical Aspects of Online Privacy*, (Technical Report), Darmstadt, 2012. URL: http://www.sit.informatik.tu-darmstadt.de/filedmin/user_upload/Group_SIT/Publications/120227a_GhSW_12.pdf [as of: 19.02.2013].

Ghostery 2012
Ghostery Main Site, 2012. URL: http://www.ghostery.com/ [12.9.12].

Goffman 1973
Goffman, E.: *The Presentation of Self in Everyday Life*, New York: The Overlook Press 1973.

Gola/Klug 2003
Gola, P./Klug, C.: *Grundzüge des Datenschutzrechts*, München: C. H. Beck, 2003, p. 4.

Google 2012 a
Google Developers: *Google Plus Platform Developer Policies*, 2012. URL: https://developers.google.com/+/policies [as of: 19.02.13].

Google 2012 b
Google Dashboard, 2012. URL: https://www.google.com/dashboard/ [as of: 19.02.13].

Google 2012 c
Google Policies & Principles : *Privacy Policy*, 2012. URL: http://www.google.com/policies/privacy/ [as of: 19.02.13].

Granovetter 1985
Granovetter, M.: "Economic Action and Social Structure: The Problem of Embeddedness". In: *American Journal of Sociology*, Vol. 91, No. 3 (Nov., 1985), Chicago, IL: The University of Chicago Press, pp. 481-510.

Gross/Acquisti 2005
Gross, R./Acquisti, A.: "Privacy and Information Revelation in Online Social Networks". In: *WEPS Ä05 Proceedings of the 2005 ACM Workshop on Privacy in the Electronic Society*: 2005, New York, NY: ACM, pp. 71-80.

Hancock/ Toma/ Ellison 2007
Hancock, J./Toma, C./Ellison, N.: "The truth about lying in online dating profiles". In: *Proceedings of the ACM Conference on Human Factors in Computing Systems* , 2007. URL: https://www.msu.edu/~nellison/hancock_et_al_2007.pdf [as of: 04.03.2013].

Hellmann 2005
Hellmann, K.: „Soziologie des Shopping. Zur Einführung". In: Hellman, K./Schrage, D. (Ed.): *Das Management der Kunden. Studien zur Soziologie des Shopping*, Wiesbaden: VS-Verlag, 2005, p. 13.

Hildebrandt 2008
Hildebrandt, M.: "Defining Profiling: A New Type of Knowledge?". In: *Profiling the European Citizen: Cros-disciplinary Perspectives*. Netherlands: Springer, 2008. pp. 17-45.

Hirschkind 2011
Hirschkind, C.: *From the blogosphere to the Street: The Role of Social Media in the Egyptian Uprising*, 2011. URL: http://www.jadaliyya.com/pages/index/599/from-the-blogosphere-to-the-street_the-role-of-social-media-in-the-egyptian-uprising [as of: 02.05.2012].

Hoeren 2011
Hoeren, T.: *Skriptum Internetrecht*, 2011. URL: http://www.unimuenster.de/Jura.itm/hoeren/materialien/Skript/Skript_Internetrecht_Oktober_2011.pdf [as of: 20.02.13].

Hornung 2011
Hornung, G.: "Datenschutz durch Technik in Europa". In: *ZD* 2011, pp. 51-6.

Hornung 2012
Hornung, G.: „Eine Datenschutz-Grundverordnung für Europa?, Licht und Schatten im Kommissionsentwurf vom 25.1.2012". In: *Zeitschrift für Datenschutz (ZD)* 3/2012, pp. 99-106.

Howison/Crowston/Wiggins 2011
Howison, J./Crowston, K. /Wiggins, A.: "Validity issues in the use of social network analysis with digital trace data". In: *Journal of the Association for Information Systems*, Vol.12, Issue 12. URL: http://crowston.syr.edu/content/validity-issues-use-social-network-analysis-digital-trace-data [as of: 20.02.13].

Ibach/Horbank 2005
Ibach, P./Horbank, M.: *Highly available location-based services in mobile environments, Service Availability*, Berlin: Springer, 2005, pp. 134-147.

Independent Centre for Privacy Protection Schleswig-Holstein 2013
Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein /Independent Centre for Privacy Protection Schleswig-Holstein: *Frequently Asked Questions about the Privacy Seal under the Data Protection Act of Schleswig-Holstein*, 2013 URL: https://www.datenschutzzentrum.de/faq/guetesiegel_engl.htm [as of: 26/02/2013].

Jandt/Roßnagel 2011
Jandt, S./Roßnagel, A.: *Datenschutz in Social Networks-Kollektive Verantwortlichkeit für die Datenverarbeitung*, ZD 2011, pp. 160-166.

Jandt/Roßnagel 2011a
Jandt, S./Roßnagel, A.: *Social Networks für Kinder und Jugendliche – Besteht ein ausreichender Datenschutz?* MMR, 2011, pp. 637, 641.

JIM 2011
JIM-Studie 2011: *Jugend, Information, (Multi-) Media: Basisstudie zum Medienumgang 12- bis 19-Jähriger in Deutschland*, 2011. URL: http://www.mpfs.de/fileadmin/JIM-pdf11/JIM2011.pdf [as of: 20.02.13].

Johnston 2012
Johnston, C.: *On Facebook, deleting an app doesn't delete your data from their system*, 2012. URL: http://arstechnica.com/gadgets/2012/05/on-facebook-deleting-an-app-doesnt-delete-your-data-from-their-system/ [as of: 18.02.2013].

Jotzo 2009
Jotzo, F.: *Gilt deutsches Datenschutzrecht auch für Google, Facebook & Co. bei grenzüberschreitendem Datenverkehr?*, MMR 2009, pp. 232-7.

Kaiser/Reichenbach 2002
Kaiser, J./Reichenbach, M.: "Evaluating security tools towards usable security", *In the Proceedings of the IFIP 17th World Computer Congress- TC13 Stream on Usability: Gaining a Competitive Edge*, Montreal: Kluwer, 2002.

Kalabis 2012
Kalabis, L./Selzer, A.: „Das Recht auf Vergessen werden nach der geplanten EU-Verordnung - Umsetzungsmöglichkeiten im Internet". In: *Datenschutz und Datensicherheit 36:9*, 2012, pp. 670-675.

Kammerl 2010
Kammerl, R./Ostermann, S.: *Medienbildung – (k)ein Unterrichtsfach? Eine Expertise zum Stellenwert der Medienkompetenzförderung in Schulen,* 2012 . URL: http://www.ma-hsh.de/cms/upload/downloads/Medienkompetenz/ma_hsh_studie_medienbildung_web.pdf [as of: 20.02.2013].

Karr-Wisniewski/Lipford/Wilson 2011
Karr-Wisniewski, P./Lipford, H./Wilson, D. "A New Social Order: Mechanisms for Social Network Site Boundary Regulation" , *In the Proceedings of the Americas Conference on Information Systems*, Detroit, MI: 2011.

Kartal-Aydemir/Krieg 2012
Kartal-Aydemir, A./Krieg, R.: *Haftung von Anbietern kollaborativer Internetplattformen – Störerhaftung für User Generated Content?*, MMR 2012, pp. 647-652.

KEIN Stuttgart 21 2012.
KEIN Stuttgart 21, 2012. URL: (http://www.facebook.com/keinstuttgart21) [as of: 02.05.2012].

Kelley et al. 2010
Kelley, P./Cesca, L./Bresee, J./Cranor, L.: "Standardizing privacy notices: an online study of the nutrition label approach". In *Proceedings of the 28th international conference on Human factors in computing systems (CHI '10)*. New York, NY: ACM pp. 1573-1582.

Konferenz der Datenschutzbeauftragten des Bundes und der Länder 2011
Konferenz der Datenschutzbeauftragten des Bundes und der Länder, Datenschutz als Bildungsaufgabe DANA Datenschutznachrichten 4/2011, pp. 159.

Kontogiannis/ Lewis/ Smith 2008
Kontogiannis, K./Lewis, G./Smith, D.: "Research Agenda for Service-Oriented Architecture", International Conference on Software Engineering, 2008. URL: http://portal.acm.org/citation.cfm?id=1370917 [as of: 02.05.2012].

Krempl 2012
Krempl, S.: *Massive Kritik an geplanter EU-Datenschutzreform*, heise online 2012. URL: http://www.heise.de/-1734457. [as of: 22.10.2012].

Krishnamurthy 2010
Krishnamurthy, B.: "I know what you will do next summer". In: *SIGCOMM Computer Communication Review*, 40, Vol. 5, 2010.

Kronauer 2010
Kronauer, M.: *Exklusion. Die Gefährdung des Sozialen im hochentwickelten Kapitalismus*, Frankfurt/M.: Campus Verlag 2010.

Kumari et al. 2011
Kumari, P./Pretschner, A./Peschla, J./Kuhn, J.: "Distributed Data Usage Control for Web Applications: A Social Network Implementation. Proc.", 1st ACM Conference on Data and Application Security and Privacy, February 2011. pp. 85-96.

Lamla 2011
Lamla, J.: „Verbraucherdemokratie: Ein Zwischenbericht zur Politik der Konsumgesellschaft". In: Heidbrink, L./Schmidt, I./Ahaus, B. (Ed.): *Die Verantwortung des Konsumenten. Über das Verhältnis von Markt, Moral und Konsum*, Frankfurt/New York: 2011 p. 96.

Lamla 2012
Lamla, J.: „Netizenship oder Alltagsökonomie? Typologische Betrachtungen über die Motivlagen und Beteiligungsmuster von Internetnutzern sowie die Zukunft digitaler Demokratie". In: Kleemann, F./Voß, G.G. (Ed.): *Arbeit und Betrieb im Web 2.0 Zum neuen Verhältnis zwischen Betrieben und Usern*. Frankfurt/New York, in press, referenced from pre-publication version, 2012 p. 10.

Laudon/Traver 2007
Laudon, K./Traver, C.: *E-commerce*, Boston, MA: Pearson/Addison Wesley, 2007.

Leimeister et al. 2009
Leimeister, J./Huber, M./Bretschneider, U./Krcmar, H.: *Leveraging crowdsourcing: activation-supporting components for IT-based ideas competition*, (Journal of Management Information Systems), ME Sharpe, Vol. 26, No. 1, 2006 pp. 197-224.

Levitt 1984
Levitt, T.:" The Globalization of Markets". In: *The McKinsey Quarterly*, Summer 1984, URL: http://www.lapres.net/levit.pdf [as of: 6.9.2012].

Lin 2008
Lin, K.: "E-commerce technology: Back to a prominent future". In: *Internet Computing, IEEE, IEEE, Piscataway*, NJ: 2008, 12, pp. 60-65.

Lipford/Besmer/Watson 2008
Lipford, H./Besmer, A./Watson, J.: "Understanding privacy settings in facebook with an audience view". In: *Proceedings of the 1st Conference on Usability, Psychology, and Security*, Berkeley, CA: USENIX Association 2008.

Liu et al. 2011
Liu, Y./ Gummadi, K./Krishnamurthy, B./ Mislove, A.: "Analyzing facebook privacy settings: user expectations vs. reality". In: *Proceedings of the 2011 ACM SIGCOMM conference on Internet measurement (IMC '11)*. New York, NY: ACM 2011.

Livingstone et al. 2011
Livingstone, S./Haddon, L./Görzig, A./Ólafsson, K.: *EU Kids Online*, 2011 URL: http://www2.lse.ac.uk/media@lse/research/EUKidsOnline [as of: 22.02.2013].

Lovat/Pretschner 2011
Lovat, E./Pretschner, A.: "Data-centric multi-layer usage control enforcement: A social network example". In: *Proceedings 16th ACM Symposium on Access Control Models and Technologies*, New York, NY: ACM, 2011 pp. 151-152.

MacKenzie 2009
MacKenzie, D.: *Material Markets. How Economic Agents Are Constructed*, Oxford: Oxford University Press 2009.

Madejski/Johnson/Bellovin 2011
Madejski, M./ Johnson, M./ Bellovin, S.: "The failure of online social network privacy settings". In: *Technical Report CUCS-010-11*, Department of Computer Science, Columbia University, 2011.

Masing 2012 a
Masing, J.: „Herausforderungen des Datenschutzes". In: *Neue Juristische Wochenschrift (NJW)* 2012, pp. 2305-2311.

Masing 2012 b
Masing, J.: „Ein Abschied von den Grundrechten". In: *Süddeutsche Zeitung (SZ)* 2012, pp. 9-10.

Mauss 1968
Mauss, M.: *Die Gabe. Die Form und Funktion des Austauschs in archaischen Gesellschaften*, Frankfurt a.M.: Suhrkamp 1968.

McAfee/Brynjolfsson 2008
McAfee, A./Brynjolfsson, E.: "Investing in the IT That Makes a Competitive Difference". In: *Harvard Business Review*, July-August, 2008.

McCarthy 2010
McCarthy, C.: *Facebook applies for ad-targeting patent.* CNET, 2010. URL: http://news.cnet.com/8301-13577_3-20021141-36.html [as of: 08.02.2013].

McKeon 2012
McKeon, M.: *The Evolution of Privacy on Facebook*, 2012. URL: http://mattmckeon.com/facebook-privacy/ [as of: 29.05.2012].

Mead 1934
Mead, G.: *Mind, Self, and Society from the Standpoint of a Social Behaviourist*, Chicago, IL: University of Chicago Press, 1934.

Meißner 2008
Meißner, S.: „Personalisierter Massenkonsum im Internet". In: Schrage, Dominik/ Friederici, Markus R. (Ed.): *Zwischen Methodenpluralismus und Datenhandel. Zur Soziologie der kommerziellen Konsumforschung*. Wiesbaden (VS), 2008.

Mellahi/Johnson 2000
Mellahi, K./Johnson, M.: "Does it pay to be a first mover in e-commerce? The case of Amazon.com". In: *Management Decision*, 38, 2000, pp. 445-452.

Miller 1998
Miller, D.: *A Theory of Shopping*. Cambridge: Polity Press 1998.

Miller 2011
Miller, D.: *Tales from Facebook*. Cambridge/Malden: Polity Press 2011.

Miller 2012 a
Miller, D.: *Das wilde Netzwerk. Ein ethnologischer Blick auf Facebook*. Frankfurt a. M: Suhrkamp Verlag 2012.

Miller 2012 b
Miller, C.: *Starbucks and Square to Team Up*, 2012. URL: http://www.nytimes.com/2012/08/08/technology/starbucks-and-square-to-team-up.html [as of: 22.02.2013].

Moos 2011
Moos, F.: *Datenschutzrecht Schnell Erfasst*. London/Berlin/New York: Springer 2011.

Moos 2012
Moos, F.: „Die Entwicklung des Datenschutzrechts im Jahr 2011". In: *Kommunikation und Recht (K&R)*, 3, 2012, pp. 151-159.

Mozilla 2012
Better Privacy Add On. URL: https://addons.mozilla.org/de/firefox/addon/betterprivacy/ [12.9.2012].

Müller 2003
Müller, G./ Eymann, T./ Kreutzer, M.: *Telematik- und Kommunikationssysteme in der vernetzten Wirtschaft*. Oldenbourg: Wissenschaftsverlag 2003.

Müller et al. 2011
Müller, G./Lowis, L./Tobisch, A.: *German E-Identity*, IIG-Hitachi Report,No. 2, 2011.

Müller et al. 2011
Müller, G./Sonehara, N./Echizen, I./Wohlgemuth, S.: *Sustainable Cloud Computing, Business & Information Systems Engineering*, Springer, 3, 2011.

Müller 2012
Müller, G. et al.: „Vertrauensinfrastruktur und Privatheit als ökonomische Fragestellung". In: Buchmann, J. (Ed.): *Internet Privacy – Eine multidisziplinäre Bestandsaufnahme/A multidisciplinary analysis* (acatech STUDIE), Heidelberg et al.: Springer Verlag 2012.

Müller/Eymann/Kreutzer 2003
Müller, G./Eymann, T./Kreutzer, M.: *Telematik- und Kommunikationssysteme in der vernetzten Wirtschaft,* Lehrbücher Wirtschaftsinformatik, Oldenbourg Verlag: 2003.

Narayanan/Shmatikov 2009
Narayanan, A./Shmatikov, V.: *De-anonymizing Social Networks*, IEEE Symposium on Security and Privacy. Washington, D.C.: 2009.

Nebel/Richter 2012
Nebel, M./ Richter, P.: "Datenschutz bei Internetdiensten nach der DS-GVO, Vergleich der deutschen Rechtslage mit dem Kommissionsentwurf". In: *Zeitschrift für Datenschutz (ZD)* 9/2012, pp. 407-411.

Nissenbaum 2011
Nissenbaum, H.: "A Contextual Approach to Privacy Online". In: *Daedalus Fall No. 4*, 2011, pp. 32-48.

Nissenbaum 2011
Nissenbaum, H.: *Privacy in Context: Technology, Policy, and the Integrity of Social Life*, Palo Alto, CA: Stanford University Press 2011.

Nolte 2011
Nolte, N.: „Zum Recht auf Vergessen im Internet – Von digitalen Radiergummis und anderen Instrumenten". In: *Zeitschrift für Rechtspolitik (ZRP)44*: 8, 2011, pp. 236-240.

Northwestern University 2009
Northwestern University: "Tracking The Digital Traces Of Social Networks." In: *ScienceDaily*, 14 Feb. 2009. URL: http://www.sciencedaily.com/releases/2009/02/090213161031.htm [as of: 25.02.2013].

OECD 1999
The Organization for Economic Co-Operation and Development: OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data,1999. URL: http://www.oecd.org/document/18/0,2340,en_2649_34255_1815186_1_1_1_1,00.html [as of: 25.02.2013].

OECD 2013
The Organization for Economic Co-Operation and Development: OECD Privacy Principles, 2013. URL: http://oecdprivacy.org/ [as of: 22.02.2013].

Office of the Data Protection Commissioner, Ireland 2011
The Office of the Data Protection Commissioner, Ireland: Report of Data Protection Audit of Facebook, 2011. URL: https://www.dataprotection.ie/documents/facebook%20report/final%20report/report.pdf [as of: 25.02.2013].

Opsahl 2010
Opsahl, K.: *Facebook's Eroding Privacy Policy:* A Timeline, 2010. URL: https://www.eff.org/deeplinks/2010/04/facebook-timeline [as of: 29.05.2012].

O'Reilly 2005
O'Reilly, T.: *What is Web 2.0*, 2005, URL: http://www.oreilly.de/artikel/web20.html [as of: 25.02.2013].

Pretschner/Lovat/Büchler 2011
Pretschner, A. /Lovat, E./Büchler, M.: "Representation-Independent Data Usage Control." In: *Proceedings of the Sixth International Workshop on Data Privacy Management*, 2011. URL: http://www22.informatik.tu-muenchen.de/fileadmin/papers/dpm11.pdf [as of: 25.02.2013].

PWC 2011
PricewaterhouseCoopers: *Datenschützen: Eine Studie zum aktuellen Stand des Datenschutzes in deutschen Großunternehmen 2011*. URL: http://www.pwc.de/de_DE/de/compliance/assets/PwC_Studie_Datenschutz_2011.pdf. [as of: 25.02.2013].

Rahman et al. 2010
Rahman, F./Hoque, M./Kawsar, F./Ahamed, S.: *Preserve your privacy with pco:* "A privacy sensitive architecture for context obfuscation for pervasive e-community based applications". In: *IEEE Second International Conference on Social Computing (SocialCom)*, 2010. pp. 41-48.

Raynes-Goldie 2010
Raynes-Goldie, K.: "Aliases, Creeping, and Wall Cleaning: Understanding Privacy in the Age of Facebook". In: *First Monday*, Volume 15, Number 1 - 4 January 2010. URL: http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/2775/2432 [as of: 08.02.2013].

Rohan/Tunguz-Zawislak/Sheffer/Harmsen 2008
Rohan, T./Tunguz-Zawislak, T./Sheffer, S./Harmsen, J.: *Network node ad targeting. U.S. Patent Application 0080162260, Assignee: Google Inc.* URL: http://patentscope.wipo.int/search/en/detail.jsf?docId=WO2008082962&recNum=1&maxRec=&office=&prevFilter=&sortOption=&queryString=&tab=PCTDescription [as of: 25.02.2013].

Roßnagel/Pfitzmann/Garstka 2001
Roßnagel, A./Pfitzmann, A./Garstka, H.: *Modernisierung des Datenschutzrechts-Gutachten im Auftrag des Bundesministeriums des Innern*, Berlin 2001.

Roßnagel/Banzhaf/Grimm 2003
Roßnagel, A./ Banzhaf, J./ Grimm, R.: *Datenschutz im Electronic Commerce*, Heidelberg: Verlag Recht und Wirtschaft, GmbH 2003.

Roßnagel 2007
Roßnagel, A.: „Datenschutz in einem informatisierten Alltag", Berlin: Friedrich-Ebert Stiftung 2007.

Roßnagel 2011
Roßnagel, A., „Das Gebot der Datenvermeidung und -sparsamkeit als Ansatz wirksamen technikbasierten Persönlichkeitsschutzes?". In: Eifert, M. / Hoffmann-Riem, W. (Ed.): *Innovation, Recht und öffentliche Kommunikation* (Sonderdruck) – Innovation und Recht IV, Berlin: Duncker & Humblot 2011.

Roßnagel 2012
Roßnagel, A.: „Datenschutzgesetzgebung, Monopol oder Vielfalt?". In: *Datenschutz und Datensicherheit (DuD)* 2012, pp. 553-555.

Roth 2008
Roth, A.: "What have we learned from Market Design?" In: *Economic Journal*, 2008. pp. 285-310.

Sackmann/Strüker 2005
Sackmann, S./Strüker, J.: *Electronic Commerce Enquete - 10 Jahre Electronic Commerce: Eine stille Revolution in deutschen Unternehmen*, Leinfelden: Konradin-IT-Verlag 2005.

Schafer/Konstan/Riedl 2001
Schafer, J./Konstan, J./Riedl, J.: "E-commerce recommendation applications". In: *Data Mining and Knowledge Discovery*, Vol. 5, No. 1/2 2001, pp. 115-153.

Schafer/Konstan/Ried 1999
Schafer, J./Konstan, J./Ried, J.: "Recommender Systems in e-Commerce". In: *EC '99 – Proceedings of the 1st ACM Conference on Electronic Commerce*, 1999. URL: http://delivery.acm.org/10.1145/340000/337035/p158-schafer.pdf?ip=141.51.138.147&acc=PUBLIC&CFID=127865815&CFTOKEN=12791856&__acm__=1342519436_5ac3a8775875d04a78aff17a5861230d [as of:25.02.2013].

Schaumann 2013
Schaumann, P.: *Ihre Datenspuren im Internet*, 2013. URL: http://www.sicherheitskultur.at/spuren_im_internet.htm#user [as of: 25.02.2013].

Scheer/Kruppke/Heib 2003
Scheer, A./Kruppke, H./Heib, R.: E-Government: *Prozessoptimierung in der öffentlichen Verwaltung*, Berlin/Heidelberg/New York: Springer, 2003.

Schelske 2008
Schelske, A.: „Transparente Märkte in interaktiven Wertschöpfungsprozessen: Synchrone Konsumforschung mit vernetzten Konsumenten". In: Schrage, Dominik/Friederici, Markus R. (Ed.): *Zwischen Methodenpluralismus und Datenhandel. Zur Soziologie der kommerziellen Konsumforschung*. Wiesbaden (VS), 2008.

Schreiber 2009
Schreiber, W.: *Bundeswahlgesetz, Kommentar* (8. Auflage), Köln 2009, § 1 BWahlG, Rn. 94.

Schroeder 2009
Schroeder, S.: Gaydar: *Your Facebook friends can reveal your sexual orientation*, 2009. URL: http://mashable.com/2009/09/21/facebook-friends-sexual-orientation/ [as of: 22.02.2013].

Sievers 2012
Sievers, B.: *Ist erlaubt, was gefällt? Urheberrechtverletzung und Verantwortlichkeit beim Social Sharing, Gewerblicher Rechtschutz und Urheberrecht. Praxis im Immaterial- und Wettbewerbsrecht* (GRUR-Prax) 10/2012, pp. 229- 231.

Simitis 2011
Simitis, S.: „Simitis 2011, § 29 BDSG, Rn. 96; dissenting opinion Schmitz". In: Hoeren/Sieber, *Teil 16.2, Rn. 214,* 2012.

Singer 2011
Singer, N.: *The Trouble with the Echo Chamber,* 2011. URL: https://www.nytimes.com/2011/05/29/technology/29stream.html. [as of: 22.02.2013].

Siri/Melchner/Wolff 2012
Siri, J./Melchner, M./Wolff, A.: "The Political Network. Parteien und politische Kommunikation auf Facebook". In: Zurawski, N./Schmidt, J./Stegbauer, C. (Ed.): *Phänomen „Facebook".* Sonderausgabe von kommunikation@gesellschaft, Jg. 13, Beitrag 6. URL: http://nbn-resolving.de/urn:nbn:de:0228-201213068 [as of: 02.05.2012].

The Smoking Gun 2007
The Smoking Gun: *College Sued Over "Drunken Pirate"* Sanctions, 2007 URL: http://www.thesmokinggun.com/documents/crime/college-sued-over-drunken-pirate-sanctions [as of: 25.02.2013].

Solove 1972
Solove, D.: *Understanding Privacy*, Cambridge, Mass.: Harvard University Press, 1972 (New Edition 2008).

Solove 2008
Solove, D.: *Understanding Privacy*, Cambridge, Mass.: Harvard University Press 2008.

Solove 2011
Solove, D. J.: *Nothing to Hide. The False Trade-Off Between Privacy and Security,* New Haven u.a.: Yale University Press 2011.

Spiekermann 2006
Spiekermann, S.: "Individual Price Discrimination – An Impossibility?". In: Kobsa, A./Chepalla, R./ Spiekermann, S. (Ed.): *Proceedings of the CHI 2006 Workshop on Privacy-Enhanced Personalization.* 2006, URL: http://www.isr.uci.edu/pep06/papers/PEP06_Spiekermann.pdf [as of: 25.02.2013].

Spindler 2012
Spindler, G.: „Persönlichkeitsschutz im Internet – Anforderungen und Grenzen einer Regulierung" Gutachten F. In: *Ständige Deputation des Deutschen Juristentages, Verhandlungen des 69. Deutschen Juristentages*. München: Verlag Beck CH 2012.

Spindler/Schuster 2011
Spindler, G./Schuster, F. (Ed.): *Recht der elektronischen Medien- Kommentar*, 2. Auflage, Verlag C. H. Beck München 2011.

Statista GmbH 2012
Statista GmbH: *E-commerce Statista-Dossier,* 2012. URL: http://de.statista.com/statistik/download_file/study-Download/NDQ3MDUuMjc4Nw==/ [as of: 25.02.2013].

Steam 2013
Steam: *Hard - & Software- Umfrage:* January 2013. URL: http://store.steampowered.com/hwsurvey [as of: 25.02.2013].

Sterritt 2005
Sterritt, R.: "Autonomic computing" In: *Innovations in systems and software engineering*, 1, 2005, pp. 79-88.

Süddeutsche 2011
Süddeutsche.de: *Hacker stehlen Millionen geheime Kundendaten*, 2011 URL: http://www.sueddeutsche.de/digital/datenklau-bei-sony-hacker-stehlen-millionen-geheime-kundendaten-1.1089569 [as of: 25.02.2013].

Süddeutsche Zeitung 2011
Süddeutsche Zeitung: *1600 Gäste, keine Gastgeberin,* 2011. URL: http://www.sueddeutsche.de/panorama/facebook-party-in-hamburg-gaeste-elf-festnahmen-drei-anzeigen-1.1105389 [as of: 05.06.2011].

Sweeney 2000
Sweeney, L.: "Uniqueness of Simple Demographics in the U.S. Population". In: *Laboratory for Int'l Data Privacy, Working Paper LIDAP-WP4*, 2000. URL: http://dataprivacylab.org/projects/identifiability/pharma1.pdf [as of: 25.02.2013].

Taz.de 2012
Taz.de: *Das geht weit über Yahoo hinaus*, 2012. URL: https://www.taz.de/400000-Datensaetze-gestohlen/!97243/ [as of: 25.02.2013].

Tor 2013
The Tor Project Inc.: *Anonymity Online*, 2013.URL: https://www.torproject.org/ [as of: 12.09.2012].

TRUSTe 2013
TRUSTe: *Internet Privacy and Security for Businesses,* 2013 URL: http://www.truste.com/ [as of: 25.02.2013].

Trust Services 2013
Trust Services: *Principles, Criteria, and Illustrations*. URL: www.webtrust.org/ [as of: 25.02.2013].

Tsai et al. 2007
Tsai, J./Egelmann, S./Cranor, L./Acquisti, A.: "The Effect of Online Privacy Information on Purchasing Behaviour: An Experimental Study". In: *The Sixth Workshop on the Economics of Information Security (WEIS 2007)*. Pittsburgh, PA, June 7-8 2007. URL: http://weis2007.econinfosec.org/papers/57.pdf [as of: 25.02.2013].

Turow/Feldmann/Meltzer 2005
Turow, J./Feldman, L./Meltzer, K.: "Open to Exploitation – America's Shoppers Online and Offline". In: *Annenberg School for Communications Departmental Papers (ASC)* 2005. URL: http://repository.upenn.edu/asc_papers/35. [as of: 08.02.2013].

Turow et al. 2009
Turow, J./King, J./Hoofnagle, C./Bleakley, A./Hennessy, M.: "Americans Reject Tailored Advertising and Three Activities that Enable It". In: *Social Science Research Network,* Vol. 104, Issue 30, 2009, pp. 1-27.

Ulbricht 2012
Ulbricht, M.: "Privacy settings in online social networks as a conflict of interests- Regulating User Behaviour on Facebook". In: Abraham, A. (Ed.): *Computational Social Networks: Security and Privacy, Series in Computer Communications and Networks*. London: Springer Verlag 2012.

van den Berg 2010
van den Berg, B./ Leenes, R.: "Audience Segregation in Social Network Sites". In: *Proceedings of the IEEE International Conference on Social Computing*, 2010, pp. 1111-1116.

Wang et al. 2011
Wang, Y./Komanduri, S./Leon, P./Norcie, G./Acquisti, A./Cranor, L.: I *Regretted the Minute I Pressed Share: A Qualitative Study of Regrets on Facebook*. 2011. URL: http://cups.cs.cmu.edu/soups/2011/proceedings/a10_Wang.pdf [as of: 03.05.2012]

Waidner et al. 2011
Waidner, M./Fischer-Hübner, S./Hoofnagle, C./Krontiris, I./Rannenberg, K.: "Online Privacy: Towards Informational Self-Determination on the Internet". In: *Dagstuhl Perspectives Workshop 11061. Dagstuhl Manifestos 1(1)*, 2011, pp. 1-20.

Weinhardt et al. 2009
Weinhardt, C./Anandasivam, A./Blau, B./Borissov, N./Meinl, T./Michalk, W./Stößer, J.: "Cloud computing–a classification, business models, and research directions". In: *Business & Information Systems Engineering*, Springer, 2009, 1, pp. 391-399.

Weiss 2008
Weiss, S.: "The Need for a Paradigm Shift in Addressing Privacy Risks in Social Networking Applications". In: *IFIP International Federation for Information Processing 262*. Boston: Springer 2008, pp. 161-171.

Westin 1967
Westin, A. F.: *Privacy and Freedom*, New York: Athenum 1967.

Whitehead 1941
Whitehead, A.: *Process and Reality:* An Essay in Cosmology, New York: Free Press 1941.

Wisniewski/Lipford/Wilson 2012
Wisniewski, P./Lipford, H./Wilson, D.: "Fighting for My Space: Coping Mechanisms for SNS Boundary Regulation". *In the Proceedings of the Conference on Human Factors in Computing Systems*, Austin, TX, May 2012.

Wisniewski/Lipford/Wilson 2011
Wisniewski, P./Lipford, H./Wilson, D.: "Interpersonal Boundary Mechanisms within Online Social Networks". Extended Abstract presented at the Conference on Human Factors in Computing Systems, Workshop on the Privacy for a Networked World: Bridging Theory and Design, Philadelphia, PA: May 2011. URL: http://pamspam.com/wp-content/uploads/2011/06/pjkwis_networked_privacy_final.pdf [as of: 25.02.2013]

Wondracek et al. 2010
Wondracek, G./Thorsten H./Kirda E./Kruegel, C.: "A Practical Attack to De-anonymize Social Network Users". In: *Proceedings of the 2010 IEEE Symposium on Security and Privacy (SP '10). IEEE Computer Society*, Washington, DC: 2010, pp. 223-238.

YouCom 2011
YouCom: *Jeder Vierte während der Arbeitszeit bei Facebook,* 2011. URL: http://www.youcom.de/sites/default/files/Facebook%20Studie%20youCom%20PM%2BInterview%20%28pdf%29.pdf [as of: 20.03.2012].

> THE FOLLOWING VOLUMES HAVE BEEN PUBLISHED IN THE SERIES "acatech STUDY" AND "acatech REPORTS AND RECOMMENDS" UP TO NOW:

Albers, A./Denkena, B./Matthiesen, S. (Ed.): *Faszination Konstruktion. Berufsbild und Tätigkeitsfeld im Wandel* (acatech STUDIE), Heidelberg et al.: Springer Verlag 2012.

Buchmann, J. (Ed.): *Internet Privacy. Eine multidisziplinäre Bestandsaufnahme / A multidisciplinary analysis* (acatech STUDIE), Heidelberg et al.: Springer Verlag 2012.

Geisberger, E./Broy, M. (Ed.): *agendaCPS – Integrierte Forschungsagenda Cyber-Physical Systems* (acatech STUDIE), Heidelberg et al.: Springer Verlag 2012.

Spath, D./Walter, A. (Ed.): *Mehr Innovationen für Deutschland. Wie Inkubatoren akademische Hightech-Ausgründungen besser fördern können* (acatech STUDIE), Heidelberg et al.: Springer Verlag 2012.

Hüttl, R. F./Bens, O. (Ed.): *Georessource Wasser – Herausforderung Globaler Wandel. Beiträge zu einer integrierten Wasserressourcenbewirtschaftung in Deutschland* (acatech STUDIE), Heidelberg et al.: Springer Verlag 2012.

Appelrath, H.-J./Kagermann, H./Mayer, C. (Ed.): *Future Energy Grid. Migrationspfade ins Internet der Energie* (acatech STUDIE), Heidelberg et al.: Springer Verlag 2012. Auch in Englisch erhältlich (als pdf) über www.acatech.de

acatech (Ed.): *Organische Elektronik in Deutschland* (acatech BERICHTET UND EMPFIEHLT, Nr. 6), Heidelberg et al.: Springer Verlag 2011. Auch in Englisch erhältlich (als pdf) über www.acatech.de

Federspiel, R./Salem, S.: *Der Weg zur Deutschen Akademie der Technikwissenschaften*. Heidelberg et al.: Springer-Verlag 2011.

acatech (Ed.): *Monitoring von Motivationskonzepten für den Techniknachwuchs.* (acatech BERICHTET UND EMPFIEHLT, Nr. 5), Heidelberg et al.: Springer Verlag 2011.

acatech (Ed.): *Wirtschaftliche Entwicklung von Ausgründungen aus außeruniversitären Forschungseinrichtungen* (acatech BERICHTET UND EMPFIEHLT, Nr. 4), Heidelberg et al.: Springer Verlag 2010.

acatech (Ed.): *Empfehlungen zur Zukunft der Ingenieurpromotion. Wege zur weiteren Verbesserung und Stärkung der Promotion in den Ingenieurwissenschaften an Universitäten in Deutschland* (acatech BERICHTET UND EMPFIEHLT, Nr. 3), Stuttgart: Fraunhofer IRB Verlag 2008. Aktualisierte Kurzfassung (2012) auch in Englisch erhältlich (als pdf) über www.acatech.de

Federspiel, R./Salem, S.: *Zur Gründungsgeschichte der Deutschen Akademie der Technikwissenschaften*, Stuttgart: Fraunhofer IRB Verlag 2007.

acatech (Ed.): *Bachelor- und Masterstudiengänge in den Ingenieurwissenschaften. Die neue Herausforderung für Technische Hochschulen und Universitäten* (acatech BERICHTET UND EMPFIEHLT, Nr. 2), Stuttgart: Fraunhofer IRB Verlag 2006.

acatech (Ed.): *Mobilität 2020. Perspektiven für den Verkehr von morgen, Schwerpunkt Straßen- und Schienenverkehr* (acatech BERICHTET UND EMPFIEHLT, Nr. 1), Stuttgart: Fraunhofer IRB Verlag 2006.

> acatech – NATIONAL ACADEMY OF SCIENCE AND ENGINEERING

acatech represents the German scientific and technological communities, at home and abroad. It is autonomous, independent and a non-profit organisation. As a working academic institution, acatech supports politics and society, providing qualified technical evaluations and forward-looking recommendations. Moreover, acatech resolves to facilitate knowledge transfer between science and industry, and to encourage the next generation of engineers. The Academy counts a number of eminent scientists from universities, research institutes and companies among its Members. acatech receives institutional funding from the national and state governments along with third-party donations and funding for specific projects. It organises symposiums, forums, panel discussions and workshops to promote new technologies in Germany and to demonstrate their potential for industry and society. acatech publishes studies, recommendations and statements for the general public. The Academy is composed of three bodies, the Members, organised in the General Assembly, the Senate, whose well-known figures from the worlds of science, industry and politics advise acatech on strategic issues and ensure dialogue with industry and other scientific organisations in Germany, and the Executive Board, which is appointed by the Members of the Academy and the Senate, and which guides the work of the Academy. acatech's head office is located in Munich while offices are also maintained in the capital, Berlin, and in Brussels.

For more information, please see www.acatech.de