> Internet Privacy

Eine multidisziplinäre Bestandsaufnahme/ A multidisciplinary analysis

Johannes Buchmann (Hrsg.)

acatech STUDIE
September 2012

acatech
DEUTSCHE AKADEMIE DER TECHNIKWISSENSCHAFTEN

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

Reihenherausgeber:
acatech – Deutsche Akademie der Technikwissenschaften, 2012

Geschäftsstelle
Residenz München
Hofgartenstraße 2
80539 München

T +49 (0) 89 / 5 20 30 90
F +49 (0) 89 / 5 20 30 99

Hauptstadtbüro
Unter den Linden 14
10117 Berlin

T +49 (0) 30 / 2 06 30 96 10
F +49 (0) 30 / 2 06 30 96 11

Brüssel-Büro
Rue du Commerce / Handelsstraat 31
1000 Brüssel
Belgien

T + 32 (0) 2 / 5 04 60 60
F + 32 (0) 2 / 5 04 60 69

E-Mail: info@acatech.de
Internet: www.acatech.de

Koordination: Dr. Karin-Irene Eiermann
Redaktion: Linda Tönskötter, Dr. Grit Zacharias
Layout-Konzeption: acatech
Konvertierung und Satz: Fraunhofer-Institut für Intelligente Analyse- und Informationssysteme IAIS, Sankt Augustin

Die Originalfassung der Publikation ist verfügbar auf www.springer.com

> INHALT

VORWORT

Das Internet ist eine der bedeutendsten technologischen Errungenschaften der Geschichte, vergleichbar mit der Erfindung des Buchdrucks und der Eisenbahn. Suchmaschinen erlauben Menschen in aller Welt Zugang zu umfassenden Informationen, die zuvor, wenn überhaupt, nur einer geringen Anzahl von Menschen zugänglich waren. Nutzer* können zum Beispiel detaillierte Informationen über Krankheiten recherchieren und so ihren Ärzten fundierte Fragen stellen. Dies kann zu einer besseren medizinischen Betreuung führen. Suchmaschinen haben dazu beigetragen, dass das Internet mit seiner Fülle an Informationen heute eine wichtige Rolle bei der Bildung und Wissensaneignung spielt. Soziale Netzwerke unterstützen die weltweite Kommunikation und Interaktion, manchmal mit bedeutenden politischen Konsequenzen. So wird zum Beispiel davon ausgegangen, dass die politischen Umwälzungen in Ägypten ohne soziale Netzwerke nicht möglich gewesen wären und dass diese Netzwerke die Verbreitung von Demokratie voranbringen können. Das Internet ist zu einem globalen Marktplatz geworden, auf dem Nutzer fast alles erwerben können: seltene Bücher und CDs, elektronische Geräte, Flugtickets, Lebensmittel und vieles mehr. Die Nutzer können Preise und Qualität von Waren und Dienstleistungen, von Elektrogeräten bis zu Hotelunterkünften, vergleichen und das beste und günstigste Angebot auswählen. Dies sind nur einige Beispiele einer dramatischen Entwicklung, die eben erst begonnen hat. Vollständig neu daran ist die Zahlungsweise: Viele der im Internet angebotenen Dienstleistungen kosten kein Geld. Stattdessen zahlen die Nutzer mit ihren persönlichen Daten, die anschließend von den Anbietern für gezielte, personalisierte Werbung und andere Geschäftszwecke verwendet werden.

Es ist nicht überraschend, dass die Reaktionen von Nutzern auf diese Entwicklung zwiespältig sind. Einerseits schätzen sie die Angebote des Internets, die es ihnen ermöglichen, ihr Wissen zu erweitern, mit Freunden aus aller Welt in Kontakt zu bleiben und von neuen Möglichkeiten der politischen Partizipation Gebrauch zu machen, um nur einige zu nennen. Andererseits sorgen sich die Nutzer um ihre Privatsphäre. Sie fragen sich, was tatsächlich mit ihren Daten geschieht und ob diese heute oder auch in der Zukunft für unvorhergesehene Zwecke missbraucht werden könnten. Sie fragen sich, ob und in welcher Weise die freie Entfaltung ihrer Persönlichkeit und ihre Möglichkeiten der demokratischen Partizipation (zum Beispiel im Rahmen von freien und geheimen Wahlen) beeinträchtigt werden könnten, wenn so viele ihrer persönlichen Daten im Internet verfügbar sind. Dieses Phänomen wird gemeinhin als das Privatheitsparadoxon bezeichnet: die Gleichzeitigkeit von Akzeptanz und Bedenken im Hinblick auf die Nutzung des Internets.

Es ist gut möglich, dass dieses Paradoxon eine optimale Entwicklung der Potenziale des Internets für Individuen, die Gesellschaft und die Wirtschaft maßgeblich beeinträchtigen könnte. Womöglich zögern Nutzer, Dienstleistungen in Anspruch zu nehmen, obwohl diese ihnen große Vorteile bringen könnten. Unternehmen sind unsicher, wie sie ihre Dienstleistungen erfolgreich im Internet vermarkten können, ohne die Privatheit ihrer Kunden zu gefährden und so deren Vertrauen zu verlieren.

Aufgrund der so großen Bedeutung von Privatheit im Internet hat acatech, die Deutsche Akademie der Technikwissenschaften, 2011 ein Projekt initiiert, das sich mit dem Privatheitsparadoxon wissenschaftlich auseinandersetzt. In dem Projekt werden Empfehlungen entwickelt, wie sich eine Kultur der Privatheit und des Vertrauens im Internet etablieren lässt, die es ermöglicht, das Paradoxon aufzulösen. Wir verwenden hier den Begriff der Privatheit. Er deutet an, dass hier nicht nur der räumliche Begriff Privatsphäre gemeint ist, sondern auch das im europäischen Kontext wichtige Konzept der informationellen Selbstbestimmung einbezogen ist.

* Die Inhalte der Publikation beziehen sich in gleichem Maße sowohl auf Frauen als auch auf Männer. Aus Gründen der besseren Lesbarkeit wird jedoch die männliche Form für alle Personenbezeichnungen gewählt. Die weibliche Form wird dabei stets mitgedacht.

Der in diesem Zusammenhang verwendete Begriff der Kultur unterstreicht, dass die Beschäftigung mit dem Privatheitsparadoxon und seiner Auflösung eine komplexe Aufgabe ist. Sie muss (mediale) Bildung und Beispiele guter Praxis (best practice) mit einer angemessenen Gesetzgebung und technologischen Lösungen verbinden. Eine solche Kultur soll es dem Nutzer ermöglichen, das für ihn angemessene Maß an Privatheit im Internet einzuschätzen und dem jeweiligen Kontext und seinen Präferenzen entsprechend festzulegen. In einer solchen Kultur sind Bildungsmaßnahmen, gute Praktiken, der rechtliche Rahmen und die Technologie so entwickelt, dass der Nutzer tatsächlich diese Wahlmöglichkeit hat.

Dieser Band legt die Ergebnisse der ersten Projektphase vor: eine Bestandsaufnahme von Privatheit im Internet aus verschiedenen Blickwinkeln. Kapitel 1 stellt die Wünsche und Befürchtungen von Internetnutzern und Gesellschaft im Hinblick auf ihre Privatheit vor. Sie wurden mithilfe sozialwissenschaftlicher Methoden untersucht. Ergänzend dazu untersucht das zweite Kapitel Privatheit im Cyberspace aus ethischer Perspektive. Das dritte Kapitel widmet sich ökonomischen Aspekten: Da viele Onlinedienstleistungen mit Nutzerdaten bezahlt werden, ergibt sich die Frage, was dies sowohl für den Nutzer und Kunden als auch für die Unternehmen bedeutet. Kapitel 4 hat einen technologischen Fokus und analysiert, wie Privatheit von Internettechnologien bedroht wird und welche technischen Möglichkeiten es gibt, um die Privatheit des Nutzers zu schützen. Selbstverständlich ist der Schutz von Privatheit im Internet nicht nur ein technisches Problem. Deshalb untersucht Kapitel 5 Privatheit aus rechtlicher Sicht.

Bei der Lektüre der fünf Kapitel wird dem Leser sofort die Komplexität der Frage von Privatheit im Internet (Internet Privacy) bewusst. Daraus folgt die unbedingte Notwendigkeit eines interdisziplinären Ansatzes. In diesem Sinne wird die interdisziplinäre Projektgruppe gemeinsam Optionen und Empfehlungen für einen Umgang mit Privatheit im Internet entwickeln, die eine Kultur der Privatheit und des Vertrauens im Internet fördern. Diese Optionen und Empfehlungen werden 2013 als zweiter Band dieser Studie veröffentlicht.

Johannes Buchmann

Professor für Informatik und Mathematik der Technischen Universität Darmstadt und Mitglied von acatech

Darmstadt, im September 2012

PREFACE

The development of the Internet is one of the most significant technological advances in history, comparable to the invention of the printing press or the railroad. Search engines allow people around the world access to comprehensive information, which previously – if at all – was only available to very few. For example, users can obtain detailed information about diseases and can ask their doctors informed questions, which may lead to better treatment. Search engines have helped to make the Internet, with its wealth of information, an essential part of education. Social networks support worldwide communication and interaction, sometimes with significant political consequences. Some argue that the political changes in Egypt would not have been possible without social networks and that such networks help to spread democracy. The Internet has become a global marketplace where users can acquire almost anything: rare books or CDs, inexpensive electronic equipment, travel tickets, food, etc. Users can compare prices and the quality of goods and services such as electronic devices, hotel accommodations or airplane tickets and can select the best and cheapest offer. These are just a few examples of a dramatic development that has only just begun. What is completely new is the means of payment: many of these services are not paid for with currency. Instead, the users pay with their personal data which is used by providers for targeted advertising and other purposes.

It is not surprising that the reaction of users to this development is ambivalent. On the one hand, they appreciate the Internet services that allow them to stay in touch with friends worldwide, to improve their education, and those which open up new opportunities for political participation, to name only a few. On the other hand, users are worried about their privacy. They wonder what is really happening with their data and whether it could be misused now or in the future. They wonder whether and how the free development of their personality and their ability to participate in democratic processes is affected when so much of their personal information is available on the Internet. This is sometimes referred to as the privacy paradox on the Internet: the coexistence of acceptance and fear with regard to Internet usage.

It is very possible that such a paradox may seriously interfere with the optimal development of the potential of the Internet for individuals, society, and the economy. Users may be reluctant to use services that could be of great benefit to them. Companies are unsure how they can offer their services successfully without compromising user privacy in an inappropriate manner, thereby losing the trust of users.

Because Internet privacy is of such great importance, in 2011 the German National Academy of Science and Engineering (acatech) launched a project that focuses on the privacy paradox. The project is developing recommendations for a culture of privacy and trust that is able to resolve this paradox. The term "culture" is used to emphasize that dealing with the privacy paradox requires a complex approach that combines education and good practices with appropriate legislation and technology. Such a culture allows users to assess and choose the appropriate degree of privacy on the Internet depending on their preferences and the respective context. In such a culture, education, good practices, law, and technology are developed in such a way that this choice becomes possible.

This volume presents the results of the project's first phase: an account of Internet privacy from different viewpoints. First, the project studied the desires and fears of users and society regarding Internet privacy using social sciences methods. This is the content of Chapter 1. Complementary to this, Chapter 2 studies privacy in the cyber world from an ethical point of view. Chapter 3 is devoted to economic aspects: as many online services are paid for with user data, the question arises of what that means for the user.

Following this, Chapter 4 has a technological focus and discusses how privacy is challenged by Internet technology and what technical possibilities exist to protect user privacy. Of course, the protection of Internet privacy is not merely a technical problem. Therefore, the fifth chapter examines the situation of privacy from a legal point of view.

When reading the five chapters, it immediately becomes apparent how complex the issue of "Internet Privacy" is and that interdisciplinary work is absolutely necessary. Accordingly, in the next phases the interdisciplinary project group will jointly develop options and recommendations for dealing with Internet privacy in a way that promotes a culture of privacy and trust for the Internet. These options and recommendations will be published in 2013 as the second volume of this study.

Johannes Buchmann

Professor of Computer Science and Mathematics at
Technische Universität Darmstadt and member of acatech

Darmstadt, September 2012

PROJEKT

> AUTOREN

- Prof. Dr. Dr. h.c. Johannes Buchmann, Technische Universität Darmstadt/acatech
- Prof. em. Dr. Rafael Capurro, ehemals 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
- Michael Eldred, Köln
- Christian Flender, Albert-Ludwigs-Universität Freiburg
- Florian Kelbert, Technische Universität München
- Daniel Nagel, Stuttgart
- Maxi Nebel, Universität Kassel
- Carsten Ochs, Technische Universität Darmstadt
- Martin Peters, Albert-Ludwigs-Universität Freiburg
- Philipp Richter, Universität Kassel
- Fatemeh Shirazi, Technische Universität Darmstadt
- Hervais Simo, Technische Universität Darmstadt
- Tobias Wüchner, Technische Universität München

> PROJEKTLEITUNG

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

> PROJEKTGRUPPE

- Prof. em. Dr. Rafael Capurro, ehemals 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
- Dr. Wieland Holfelder, Google Germany
- Dr. Göttrik Wewer, Deutsche Post DHL
- Michael Bültmann, Nokia
- Dirk Wittkopp, IBM Deutschland

> AUFTRÄGE / MITARBEITER

Albert-Ludwigs-Universität Freiburg
- Christian Flender

Technische Universität Darmstadt
- Carsten Ochs
- Fatemeh Shirazi
- Hervais Simo

Technische Universität München
- Florian Kelbert

Universität Kassel
- Maxi Nebel
- Philipp Richter

Unabhängig
- Daniel Nagel, Stuttgart
- Michael Eldred, Köln

> PROJEKTKOORDINATION

Dr. Karin-Irene Eiermann, acatech Geschäftsstelle

> PROJEKTLAUFZEIT

07/2011 – 06/2013

> FINANZIERUNG

Das Projekt wurde vom Bundesministerium für Bildung und Forschung (BMBF) gefördert (Förderkennzeichen 01BY1175).

GEFÖRDERT VOM

Bundesministerium
für Bildung
und Forschung

Projektträger: Projektträger im Deutschen Zentrum für Luft- und Raumfahrt (PT-DLR), Kommunikationstechnologien

acatech dankt außerdem den folgenden Unternehmen für ihre Unterstützung:

Google Germany
Deutsche Post
Nokia
IBM Deutschland

1 UN/FAIRE INFORMATIONSPRAKTIKEN: INTERNET PRIVACY AUS SOZIALWISSENSCHAFTLICHER PERSPEKTIVE

CARSTEN OCHS, MARTINA LÖW

ZUSAMMENFASSUNG

In den aktuellen Debatten zum Status der Privatheit im Internet herrscht weitestgehend Einigkeit darüber, dass wir derzeit eine Transformation der Privatheit bezeugen. Diese Annahme adressieren wir als sozialwissenschaftliche Forschungsfrage: Lässt sich ein Wandel, gar ein Verschwinden des Privatheitsverständnisses konstatieren? Und worin genau besteht die Privatheitsproblematik im Internet? Ein Verständnis der Privatheitsvorstellungen von Nutzern und Experten für die technisch-rechtliche Infrastruktur des Internets ist unerlässlich, sollen Empfehlungen zur Entwicklung einer Vertrauenskultur im Internet formuliert werden. Um die oben genannten Fragen zu beantworten, legen wir eine theoretisch eingebettete Fokusgruppen-Studie vor, in deren Rahmen drei Nutzergruppen und eine Expertengruppe in vier Städten befragt wurden. Dabei wurde deutlich, dass das grundsätzliche Problem derzeitiger Informationspraktiken darin besteht, dass die Praktiken der Nutzer für die Betreiber der hochkomplexen soziotechnischen Strukturen zunehmend transparent werden, während umgekehrt genau das Gegenteil der Fall ist. Um dieser mangelnden Fairness beizukommen, legen wir abschließend zehn zu diskutierende Vorschläge zur Adressierung der Problematik vor.

ABSTRACT

It is a widely-held belief in current debates about Internet privacy that we are witnessing an absolute transformation of the conception and perception of privacy. It is this supposition that we will address in our research, asking: is there a change in societal ideas of privacy?; is the idea of privacy disappearing completely? And what exactly is the problem with privacy on the Internet? We need a deep understanding of the notions of privacy held by users as well as experts if we are to enunciate recommendations for developing a culture of privacy and trust on the Internet. In order to address the questions presented above, we are presenting a theoretically-framed focus group study which was conducted in four cities, and included three distinct user groups and one group of experts. Our research indicates that the basic problem is the unfairness of contemporary information practices: while users' practices are becoming increasingly transparent to the gaze of providers, the providers' practices disappear from view. We will present ten suggestions for rendering information practices more fair.

1.1 EINFÜHRUNG

Von Anfang an verbindet sich mit dem Aufkommen von Informations- und Kommunikationstechnologien die Sorge, dass die Nutzung dieser Technologien eine Schwächung oder Erosion von Privatheit hervorrufen würde. Es verwundert also wenig, dass seit einigen Jahrzehnten in regelmäßigen Abständen das „Ende der Privatheit" ausgerufen wird.[1] Bei allen Unterschieden in der Bewertung sind sich die diversen Beobachter zumindest dahingehend einig, dass die Entwicklung, Verbreitung und fortdauernde Evolution des Internets sowie darauf bezogener Anwendungen und Technologien massive Transformationen hinsichtlich des Privaten mit sich bringt. Von „gläsernen Bürgern" ist die Rede, von der „transparenten Gesellschaft" oder von „Daten-Exhibitionismus." Zudem wird gern darauf verwiesen, dass gerade jüngere Internetnutzer persönliche Informationen freiwillig und in vollendeter Fahrlässigkeit den wirtschaftlichen und staatlichen „Datenfressern"[2] überließen. Dass die jungen Leute gar keinen Begriff mehr von Privatheit haben und die älteren ihre Privatsphäre nicht mehr unter Kontrolle, davon berichten Stammtischdebatten, politische Sonntagsreden und Feuilletons gleichermaßen.

Im Rahmen des Projektes *Internet Privacy* geht es darum, eine differenzierte Analyse des wahlweise beklagten oder gefeierten Phänomens durchzuführen. Für eine solche Analyse ist es von entscheidender Bedeutung, die angeführten Positionen zunächst als Anlass zu begreifen, das Phänomen empirisch zu untersuchen. Aufgabe des sozialwissenschaftlichen Projektanteils ist es dabei, die Frage zu stellen, ob sich das Verständnis von Privatheit tatsächlich völlig gewandelt oder gar aufgelöst hat. Die empirische Tatsache, dass 60 Prozent der deutschen Bürger Zweifel an der Sicherheit des Internets haben und insbesondere eine Überwachung oder Ausspähung der eigenen Privatsphäre fürchten,[3] spricht ja keineswegs für ein Auflösen von Privatheitsvorstellungen. Liegt aber möglicherweise ein Wandel vor? Und welche Befürchtungen hegen Internetnutzer genau? Wie gehen sie mit diesen Befürchtungen bei der Nutzung um? Würden sie sich bessere Möglichkeiten wünschen, Dinge im Internet privat zu halten? Ein Verständnis der Privatheitsvorstellungen und -praktiken sowohl verschiedener Nutzergruppen als auch derjenigen Akteure, die an der Bildung der technischen und rechtlichen Infrastruktur des Internets mitwirken (IT-Sicherheitsunternehmen, Datenschützer), ist für das Erreichen des Projektzieles unerlässlich. Denn nur wenn diese bekannt sind, können Empfehlungen hinsichtlich der Entwicklung einer Kultur des Vertrauens im Internet gemacht werden.

In diesem Kapitel wird die sozialwissenschaftliche Bearbeitung der oben genannten Fragen dokumentiert. Um die Fragen überhaupt mit sozialwissenschaftlichen Mitteln bearbeitbar zu machen, werden zunächst allgemeine Grundzüge sozialwissenschaftlicher Privatheitstheorie herausgearbeitet (1.2). Diese Grundzüge werden dann an die interdisziplinäre Diskussion um soziotechnische Privatheit angeschlossen. Auf diese Weise wird das theoretische Feld abgesteckt, in das die verwendete Forschungsheuristik eingebettet werden muss (1.3). Daraufhin erfolgt eine Entfaltung der Forschungsheuristik (1.4) und deren Operationalisierung im Forschungsdesign (1.5). Im nächsten Schritt werden die so erarbeiteten Forschungsresultate aufgeführt und erste Folgerungen abgeleitet (1.6). Wir schließen mit einer Diskussion der identifizierten Problemlagen und legen abschließend zehn Vorschläge zur Entwicklung einer Kultur der Privatsphäre und des Vertrauens im Internet vor (1.7).

---

1 Vgl. dazu Solove 2008, S. 4. Dort werden auch einschlägige Veröffentlichungen aus mehreren Jahrzehnten angeführt. Die Ära der „Post-Privacy" wurde vor etwa zehn Jahren von Joshua Meyrowitz – durchaus mit kritischem Impetus – prognostiziert, vgl. Meyrowitz 2002. Aktuell verbindet man mit diesem Begriff wahrscheinlich eher die affirmativen Prophezeiungen der sogenannten „Post-Privacy-Bewegung", vgl. Heller 2011; eine kritisch-konstruktive Auseinandersetzung mit der aktuellen Lage legen dagegen zwei Vertreter des Chaos Computer Clubs vor, vgl. Kurz / Rieger 2011.

2 Kurz / Rieger 2011.

3 Dörflinger 2009.

1.2 PRIVATHEIT ALS THEMA DER SOZIALWISSENSCHAFTEN

Die Sozialwissenschaften des 20. Jahrhunderts haben dem Thema „Privatheit" recht wenig Aufmerksamkeit geschenkt. Folgerichtig konstatierte der britische Soziologe Joe Bailey vor etwas mehr als einem Jahrzehnt eine „under-theorisation of the private in sociological thought."[4] Und einer der führenden (interdisziplinären) Privatheitstheoretiker schrieb auch Ende des ersten Jahrzehnts der 2000er Jahre noch: „Privacy [...] is a concept in disarray. Nobody can articulate what it means."[5] Wie ein Blick in die diversen soziologischen Wörterbücher und *Dictionaries* verdeutlicht, lässt sich diese Diagnose mit Leichtigkeit auf die deutschsprachigen Sozialwissenschaften übertragen. Entweder fehlt der Eintrag „Privatheit" dort gänzlich;[6] oder es werden nur sehr kurze und grobe Bestimmungen geliefert.[7] Die ausführlichsten Erläuterungen finden sich noch in englischsprachigen Wörterbüchern[8] – und dies trotz der Tatsache, dass einflussreiche liberale Denker der englischsprachigen Tradition, wie etwa John Locke oder John Stuart Mill, der Thematik keine einzige Zeile widmeten.[9]

In der soziologischen Literatur erscheint Privatheit zumeist als die eine Seite der Unterscheidung „Öffentlich(keit) / Privat(heit)." Die *Herkunft* dieser Unterscheidung wird in den jeweiligen Bestimmungen allerdings auf verschiedene historische Situationen zurückgeführt. Einige Autoren sehen sie mit der Entstehung der Industriegesellschaft oder des Kapitalismus ab Ende des 18. Jahrhunderts einhergehen.[10] Zwei dichotom und kategorial getrennte Bereiche hätten sich damals ausgebildet: Die Öffentlichkeit der Arbeitswelt und die Privatsphäre der Familie, wobei die Trennlinie zwischen den Sphären „ge-gendered" worden sei (männliche Öffentlichkeit / weibliche Privatsphäre). Die empirische Stichhaltigkeit der Behauptung der Trennlinie wurde jedoch mitunter als ideologisches Konstrukt kritisiert, oder es wurde zumindest die Stabilität und Statik der Grenzziehung infrage gestellt, so zum Beispiel von Vertretern des Feminismus.[11]

Ein zweiter historischer Ausgangspunkt für die Entstehung der Unterscheidung von Öffentlichkeit und Privatheit wird bereits in der griechischen Antike verortet.[12] Auch diese Verortung ist mit der Behauptung verbunden, dass mit Entstehen der Unterscheidung eine normative Privilegierung der Sphäre der Öffentlichkeit einhergegangen sei: Die Akteure der Privatsphäre wären (ähnlich der Argumentation zu „Öffentlichkeit / Privatheit-in-der-Industriegesellschaft") vornehmlich Frauen, Kinder und Sklaven, Ansehen sei jedoch ausschließlich im Bereich der nur Männern zugänglichen Öffentlichkeit zu erwerben gewesen – eben deshalb habe der öffentliche Bereich in den patriarchalischen Gesellschaften der griechischen Antike mehr gegolten als der private (die negative Konnotation des Begriffes „deprivation" vermittle davon eine Ahnung, weise sie doch denselben Wortstamm wie der Begriff „privat" auf[13]). Verschiedene Kommentatoren legen den Gedanken nahe, dass einige der im weiteren Sinne sozialwissenschaftlichen Literaturklassiker diese normative Privilegierung des Öffentlichen durch (mehr oder minder ausdrückliche) Referenz auf die griechische Antike gleichsam

4 Bailey 2000, S. 382.
5 Solove 2008, S. 1.
6 Bernsdorf 1969; Boudon / Bourricaud 1989; Endruweit / Trommsdorff 1989; Endruweit / Trommsdorff 2001.
7 Jary / Jary 1991; Reinhold / Lamnek / Recker 2000; Hillmann 2007.
8 Zum Beispiel Marx in Ritzer 2007; Turner 2006.
9 Introna 1997, S. 261.
10 So Hillmann 2007; Reinhold / Lamneck / Recker 2000.
11 Vgl. Jary / Jary 1991.
12 Bailey 2000; Turner 2006.
13 So schreibt Turner: „The private arena was associated with deprivation (*privatus*), while the public sphere was one of freedom and reason, where citizens congregated for political debate and economic exchange." Turner 2006, S. 474.

unter der Hand importiert hätten.[14] Im Resultat habe sich die Soziologie des 20. Jahrhunderts vordringlich mit einem normativ positiv bewerteten Öffentlichkeitskonzept auseinandergesetzt und dann oftmals empirische Verlustgeschichten dieser Öffentlichkeit geschrieben.[15]

In der Soziologie ist nun spätestens seit den 1990er Jahren ein verstärktes Interesse an der Kategorie der Privatheit auszumachen,[16] was mit einigem Recht auf das Aufkommen und die Verbreitung digitaler Technologien zurückzuführen sein dürfte.[17] Die hier präsentierte Forschung reiht sich in dieses technologisch induzierte, wiedererwachte soziologische Interesse an der Privatheitsthematik ein. Wie wir weiter unten ausführlich darlegen werden, geht es uns um eine sozialwissenschaftliche Erforschung des Phänomens *Internet Privacy*. Und um eine solche Forschung durchführen zu können, müssen wir freilich mit einem dem empirischen Fall angemessenen Privatheitskonzept arbeiten. Nun hat sich die Formulierung einer allumfassenden Theorie der Privatheit, welche die „Essenz des Privaten" in abstrakten Termini Kontext-enthoben artikuliert, in den letzten Jahrzehnten als zum Scheitern verurteilt erwiesen.[18] Uns wird es hier deshalb nicht um die Entwicklung einer soziologischen Theorie *der* Privatheit gehen, sondern um ein pragmatisches Vorgehen – um die Ausarbeitung einer Forschungsheuristik, mit der sich *Internet Privacy* soziologisch untersuchen lässt. Eine terminologische Bestimmung von Privatheit ist jedoch auch dafür unerlässlich. Um uns einer solchen anzunähern, werden wir in einem ersten Zugriff fünf allgemeine Charakteristika sozialwissenschaftlicher Privatheitstheorie herausarbeiten und vorstellen. Diese Charakteristika müssen und werden in der weiter unten dargelegten Forschungsheuristik dann auch Berücksichtigung finden.

1.2.1 CHARAKTERISTIKA SOZIALWISSENSCHAFTLICHER PRIVATHEITSTHEORIEN

Als erste Annäherung an das Privatheitskonzept werfen wir also zunächst einen Blick auf die sozialwissenschaftliche Theoriebildung. Trotz der eher stiefmütterlichen Behandlung der Privatheitsthematik finden sich in den Sozialwissenschaften vier Ansätze, die nicht nur zur Entwicklung des Konzeptes einiges beitragen können, sondern die zudem auch immer wieder in den aktuellen Diskussionen um technologisch erzeugte Privatheit im Sinne von Vorläufern herangezogen werden: Georg Simmels Überlegungen zum Geheimnis; Erving Goffmans Theorie des Selbst im Alltag; Alan Westins Behandlung des Zusammenhangs von Privatheit und Freiheit sowie schließlich die sozialpsychologische Privatheitskonzipierung Irwin Altmans. Eine vergleichende Betrachtung dieser Theorien ermöglicht eine Ausweisung der Grundzüge des sozialwissenschaftlichen Nachdenkens über Privatheit. Eben diese Grundzüge werden wir im Folgenden vorstellen.[19]

Privatheit als Kontrolle persönlicher Informationen und als Regulierung des Zugangs zum Selbst

Das in der soziologischen und anthropologischen Literatur vorzufindende Verständnis von Privatheit lässt sich zunächst grob in zwei Klassen einordnen:

---

14 „Etymologically the word *private* signifies deprivation, bereftness, dispossession. The sense of withdrawal and separation, restriction, seclusion is clear in early usages. *Public* thus has a revealing linguistic priority – or at any rate a positively charged quality – which clearly meshes with and underwrites the privileged status of the collective, the communal and the civic within the social disciplines." Bailey 2000, S. 397.

15 So zum Beispiel Arendt 1951; Habermas 1962; Sennett 1983.

16 Bailey 2000, S. 381.

17 Vgl. dazu Marx 2001.

18 Vgl. Solove 2008, S. 8-9; Nissenbaum 2010, S. 2-3.

19 Natürlich finden sich auch bei anderen im weiteren Sinne sozial- und kulturwissenschaftlichen Denkern Anregungen zur Entwicklung eines Privatheitskonzeptes, so etwa bei Marx, Durkheim, Weber und Tocqueville oder bei den Autoren der Frankfurter Schule, bei Freud, Foucault und im Feminismus, s. dazu Bailey 2000, S. 386-389. Wir konzentrieren uns hier zunächst aus den oben genannten Gründen (zum Teil explizite Auseinandersetzung mit Privatheit, zudem expliziter Bezug auf diese Theorie in der aktuellen Literatur) auf die oben genannten Autoren. Auf einige der hier zunächst ausgelassenen Theorien werden wir im weiteren Textverlauf dann jedoch noch Bezug nehmen.

– Privatheit als die Möglichkeiten, über die ein Individuum verfügt, um ihre oder seine persönlichen Informationen zu kontrollieren; und:
– Privatheit als Regulierung des Zugangs zum Selbst einer Person.[20]

Georg Simmel wies bereits Anfang des 20. Jahrhunderts darauf hin, dass die Ausbildung einer Beziehung notwendig ein Mindestmaß an Wissen – oder eben Information – aber auch an Nicht-Wissen bezüglich des Gegenübers voraussetze. Simmels Überlegungen sind insofern jenen Ansätzen zuzuordnen, die Privatheit als Informationskontrolle konzipieren,[21] als bei Simmel das für eine Beziehung legitime und adäquate Maß an Wissen und Nicht-Wissen deren Qualität definiert: „Alle Beziehungen von Menschen untereinander ruhen selbstverständlich darauf, daß sie etwas voneinander wissen."[22] Jedoch gelte gleichermaßen, dass

> *„man niemals einen andren absolut kennen kann, – was das Wissen um jeden einzelnen Gedanken und jede Stimmung bedeuten würde, – da man sich aber doch aus den Fragmenten von ihm, in denen allein er uns zugänglich ist, eine personale Einheit formt, so hängt die letztere von dem Teil seiner ab, den unser Standpunkt ihm gegenüber uns zu sehen gestattet."*[23]

Folglich ergebe sich aus dem Zusammenspiel von Wissen und Nicht-Wissen die Form jeweiliger Beziehungen:

> *„das Wissen umeinander, das die Beziehung positiv bedingt, tut dies nicht schon für sich allein – sondern, wie sie nun einmal sind, setzen sie ebenso ein gewisses Nichtwissen, ein freilich unermeßliches wechselndes Maß gegenseitiger Verborgenheit voraus."*[24]

In eine ganz ähnliche Richtung gehen die Überlegungen Erving Goffmans, der seinen Ansatz ausdrücklich in großer Nähe zur Simmelschen Soziologie verortet.[25] Grundsätzlich ging es Goffman in seinen Interaktionsstudien darum, die Rollen zu analysieren, die Menschen im Alltag für unterschiedliche Publika spielen, um so ihr Selbst zu entwerfen. Das Rollenspiel diene dem Zweck, die Preisgabe individueller Informationen zu kontrollieren:

> *„When an individual enters the presence of others, they commonly seek to acquire information about him or to bring into play information about him already possessed. […] Information about the individual helps to define the situation, enabling others to know in advance what he will expect of them and what they may expect of him. Informed in these ways, the others will know how best to act in order to call forth a desired response for him."*[26]

Beziehungen gründen sich in diesem Sinne sowohl für Simmel als auch für Goffman auf Wissen beziehungsweise auf Information; die Qualität einer Beziehung wird (zumindest

---

20 Unsere vergleichende Betrachtung sozialwissenschaftlicher Privatheitstheorien befindet sich an diesem Punkt in Übereinstimmung mit der Klassifizierung verschiedenster Privatheitstheorien nach Zugang und Kontrolle durch Helen Nissenbaum, vgl. Nissenbaum 2010, S. 69-71; vgl. auch Introna 1997, S. 262-263. Daniel J. Solove nimmt dahingegen eine wesentlich feinkörnigere Unterteilung vor, derzufolge die verschiedenen Privatheitstheorien auf folgende Bereiche fokussieren: „The Right to Be Let Alone", „Limited Access to the Self", „Secrecy", „Control over Personal Information", „Personhood" und „Intimacy", vgl. Solove 2008, S. 15-37. Da wir keine allgemeingültige Privatheitsdefinition vorlegen wollen, sondern das bescheidenere Ziel verfolgen, eine zur Erforschung des Phänomens *Internet Privacy* angemessene Forschungsheuristik zu entwickeln, ist die Einordnung von Privatheitstheorien nach Kontrolle und Zugang dennoch pragmatisch gerechtfertigt.

21 „Simmel's thinking about secrecy as a means of information control can help us understand new forms of sociation emerging in a rapidly developing information society." Marx / Muschert 2009, S. 229.

22 Simmel 1992, S. 383.

23 Simmel 1992, S. 384.

24 Simmel 1992, S. 391.

25 Goffman 1973, S. XII.

26 Goffman 1973, S. 1.

teilweise) vom Grad an Informationen festgelegt, über die die Individuen verfügen. Was in Beziehungen verborgen – das heißt privat – bleibt, bestimmt sich dabei über die Informationen, die nicht preisgegeben werden. Kontrolle über die eigene Privatheit meint in diesem Sinne Kontrolle über persönliche Informationen.

Am ausdrücklichsten vertrat wohl Alan Westin ein ebensolches Privatheitsverständnis. Es mündet in folgendem berühmten Zitat:

> *„Privacy is the claim of individuals, groups or institutions to determine for themselves when, how, and to what extent information about them is communicated to others. [...] The individual's desire for privacy is never absolute, since participation in society is an equally powerful desire. Thus each individual is continually engaged in a personal adjustment process in which he balances the desire for privacy with the desire for disclosure and communication for himself."*[27]

Das Bedürfnis nach Privatheit ist bei Westin allerdings kein absolutes, sondern steht in einem Spannungsverhältnis zum Bedürfnis nach Sozialität. Genau diese Dichotomisierung wurde vielfach kritisiert, weil daraus folge, dass eine Situation perfekter Privatheit (Westin nennt dies „solitude"[28]) bei Westin letztlich nicht mehr als soziale Situation erscheine:[29] Das Privatheitskonzept werde von ihm am Vorbild des Individuums entwickelt,[30] woraus wiederum Probleme entstünden (auf die wir weiter unten noch zu sprechen kommen werden).

Eine Reihe von Kommentatoren sind nun der Auffassung, dass der Westin'sche Individualismus bei Irwin Altman, einem anderen einflussreichen Privatheitstheoretiker, vermieden wird. Altman erreiche dies, indem er von vornherein nicht die Kontrolle individueller Informationen, sondern vielmehr den Zugang zum Selbst einer Person zentral stelle.[31] Altmans Privatheitsdefinition lautet wie folgt:

> *„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."*[32]

Privatheit gilt bei Altman also *immer* als „interpersonal event, involving relationships among people."[33]

Privatheitskonzeptionen sind folglich auf den ersten Blick nach Informationskontrolle und Zugang-zum-Selbst voneinander abgrenzbar, bei genauerer Betrachtung verliert diese Unterscheidung jedoch an Gewicht. So geht Altman beispielsweise davon aus, dass das Ziehen von Interaktionsgrenzen auf „Control of Input from Others" und „Control of Output to Others" abziele.[34] Zur Regulierung des Zugangs-zum-Selbst würden Interaktionsgrenzen gezogen und diese dienten ihrerseits der Kontrolle eingehender und ausgehender Informationen („Input" beziehungsweise „Output"). Informationskontrolle und Zugang-zum-Selbst fallen somit bei Altman letztlich in eins – und dies gilt nun für alle der hier behandelten Ansätze: Wissen/Nicht-Wissen bestimmt für Simmel eine soziale Beziehung, auf letzterer beruhen wiederum die Interaktionsoptionen und -grenzen zwischen

27 Westin 1967, S. 7.
28 Westin 1967, S. 31.
29 Vgl. die Kritik in Steeves 2009.
30 Margulis 2003b, S. 418.
31 In eben diesem Sinne Steeves 2009.
32 Altman 1975, S. 6.
33 Altman 1975, S. 22.
34 Altman 1975, S. 29.

Individuen;[35] Goffman lässt sich dahingehend interpretieren, dass Privatheit die Regulierung des Zugangs-zum-Selbst meint, welche ihrerseits erfolgt, um die Informationen dieser Person kontrollieren zu können;[36] und auch bei Westin finden sich unterschiedliche Grade des Zugangs-zum-Selbst, welche mit dem Maß an preisgegebener persönlicher Information in Zusammenhang stehen.[37] Zu dieser Diagnose passt auch die Beobachtung, dass sich in den zeitgenössischen Kommentaren zu den vier klassischen Privatheitstheorien ein ständiges Changieren zwischen Zugang und Kontrolle findet. Während sich die Kommentatoren mitunter über ihre eigene Privatheitsdefinition zunächst einem der Ansätze ausdrücklich zuordnen, schaffen sie es kaum, diese Zuordnung durchzuhalten. Gary T. Marx arbeitet beispielsweise mit einem von Simmel abgeleiteten Konzept der Informationskontrolle,[38] schreibt aber:

> *„I am interested in the impact of technology on the borders between the self and others and the conditions under which personal information borders are seen to be legitimateley and illegitimateley crossed."*[39]

Die Kontrolle persönlicher Informationen und der Zugang zum Selbst sind in diesem Sinne höchstens analytisch trennbar, empirisch fallen sie zusammen, oder genauer: „The control-over-information conception can be viewed as a subset of the limited-access conception."[40] Ein wenig vorgreifend halten wir fest: Da es uns hier um technologisch erzeugte Privatheit gehen wird, verstehen wir Privatheit ganz in diesem Sinne als Informationskontrolle und gleichzeitig als Zugang-zum-Selbst.

Privatheit als Bestandteil aller sozialen Beziehungen und als soziale Konstruktion

Privatheit kann zudem ganz grundsätzlich als soziales Phänomen gelten.[41] Simmel zufolge enthält jede Beziehung einen Rest an Nicht-Wissen bezüglich des Gegenübers, *jede* Beziehung weist also einen gewissen Privatheitsbereich auf. Er argumentiert diesbezüglich gleichsam kantianisch im Sinne einer unvollständigen Erkennbarkeit von Welt. Darin, dass unser Wissen um Andere stets und notwendig unvollständig bleibe, drücke sich nicht bloß ein kognitiver Mangel von Beobachtern aus; vielmehr stelle diese Unvollständigkeit ein *soziales Erfordernis* dar: „es ist überhaupt kein andrer Verkehr und keine andre Gesellschaft denkbar, als die auf diesem teleologisch bestimmten Nichtwissen des einen um den andren beruht."[42] Das Nicht-Wissen gilt Simmel somit nicht als Defizit, sondern als notwendiger, vom sozialen Gefüge konstruierter und respektierter Bereich, in den nicht eingedrungen werden soll. Dementsprechend ist Simmel der Auffassung, „daß um jeden Menschen eine ideelle Sphäre liegt, nach verschiedenen Richtungen und verschiedenen Personen gegenüber freilich ungleich groß, in die man nicht eindringen kann, ohne den Persönlichkeitswert des Individuums zu zerstören."[43]

Auch Goffman setzt mit der Überlegung an, dass Beobachter Andere nie völlig ergründen könnten. Deshalb müssten sie sich auf die Interpretation von ausgesendeten Zeichen verlassen. Beobachtete gäben ihrerseits *nolens volens* Informationen über sich preis (kommunizierten also) – und zwar selbst dann, wenn sie sich „lediglich verhielten."[44] Alle Akteure seien sich dessen normalerweise bewusst. Aus diesem Grund versuchten sie, die Preisgabe von Informationen zu

35 Simmel 1992, S. 396.
36 Goffman 1973, S. 2 und S. 134-137.
37 Westin 1967, S. 31-32.
38 Marx / Muschert 2009, S. 229.
39 Marx 2001, S. 157.
40 Solove 2008, S. 25.
41 Margulis 2003a.
42 Simmel 1992, S. 388.
43 Simmel 1992, S. 396.
44 Vgl. Gofffman 1973, S. 2.

kontrollieren,[45] indem sie vor anderen Performances aufführten. Gleichermaßen bräuchten die Akteure auch Rückzugsmöglichkeiten, sogenannte „backstage regions", wo sie ihre Performances planten und vom Rollenspiel zeitweise befreit wären. Das Publikum würde üblicherweise daran mitarbeiten, diese Rückzugsmöglichkeiten aufrechtzuerhalten, es würde sich diskret und taktvoll verhalten – der Backstage-Bereich werde in diesem Sinne sozial konstruiert.[46]

Alan Westin diskutiert Privatheit indes als evolutionsgeschichtlich konstantes Phänomen, das sich auf die gesamte zoologische Welt erstrecke,[47] weshalb Privatheit notwendiger Bestandteil aller Sozialitätsformen sei: „the individual in virtually every society engages in a continuing personal process by which he seeks privacy at some times and companionship at other times."[48] Folgerichtig konstatiert Valerie Steeves: „Westin's understanding of privacy is rich in sociality."[49] Dies werde insbesondere an den vier grundsätzlichen Privatheitsmodi deutlich, die Westin anführt. Neben der schon erwähnten (und kritisierten) individuellen Isolation („solitude") sind dies: Die Intimität mehrerer, die Anonymität-in-der-Öffentlichkeit und die einem Individuum von einer umgebenden Gruppe zur Verfügung gestellten psychologischen Barrieren zur Kommunikationsbeschränkung, „reserve" genannt.[50]

Irwin Altman gründet sein Privatheitskonzept von vornherein auf einer „Social-Systems"-Perspektive.[51] Er geht davon aus, dass Privatheit unterschiedliche Grade annehmen und unter Einsatz verschiedener Mechanismen erreicht werden kann (zum Beispiel verbal, unter Rückgriff auf Architektur, Kleidung, Normen usw.[52]). Die Mechanismen und die resultierenden Verhaltensweisen bildeten ein dynamisches System zur Regulierung von Privatheit, welche Altman nicht als gegebenen statischen Zustand, sondern als in sozialen Beziehungen jeweils ausgehandeltes Verhältnis bestimmt. Privatheit ist damit insofern als etwas zutiefst Soziales zu verstehen, als sie immer *in Beziehungen* konstruiert wird. Darin deutet sich schon das nächste Charakteristikum an.

Privatheit: Anthropologisch universell, aber kulturhistorisch kontingent

Anfang des 20. Jahrhunderts wunderte sich Georg Simmel über

> *„die soziologisch höchst eigentümliche Beziehung, die man in den höheren Kulturschichten jetzt als die ‚Bekanntschaft' schlechthin bezeichnet. Daß man sich gegenseitig ‚kennt', bedeutet in diesem Sinne durchaus nicht, daß man sich gegenseitig kennt, d. h. einen Einblick in das eigentlich Individuelle der Persönlichkeit habe; sondern nur, daß jeder sozusagen von der Existenz des andren Notiz genommen habe."*[53]

Die Bekanntschaft gilt Simmel aufgrund der Neuheit des Beziehungstypus, den sie darstellt, nicht nur als Beispiel für das jeweils neuartige Mischungsverhältnis von Wissen und Nicht-Wissen historischer Sozialitätstypen, sondern auch als Nachweis dafür, dass sich „die Verhältnisse an der Frage des Wissens umeinander [scheiden]".[54] Privatheit ist mit anderen Worten kulturhistorisch kontingent: Das adäquate Maß an Wissen/Nicht-Wissen in einer Beziehung wird von der zu einem bestimmten historischen Zeitpunkt in einer Sozialformation vorherrschenden Kultur bestimmt.

45 Goffman 1973, S. 8.
46 Goffman 1973, S. 106-140.
47 Westin 1967, S. 8-11.
48 Westin 1967, S. 13.
49 Steeves 2009, S. 196.
50 Westin 1967, S. 31-32.
51 Altman 1975, S. 4.
52 Altman 1975, S. 31-42.
53 Simmel 1992, S. 395.
54 Simmel 1992, S. 396.

Die historisch wandelbare Privatsphäre umgebe Menschen zu unterschiedlichen Zeiten *in unterschiedlicher Weise* – als anthropologische Universalie umgebe sie sie aber *immer*. Das zeige sich auch am historischen Wandel der Freundschaftsverhältnisse seit der Antike von der Idee völliger Vertrautheit hin zu „differenzierten Freundschaften [...] d. h. zu solchen, die ihr Gebiet nur an je einer Seite der Persönlichkeiten haben und in die die übrigen nicht hineinspielen."[55] Den vorläufigen Endpunkt dieser Entwicklung sah Simmel Anfang des 20. Jahrhunderts dann im Aufkommen des großstädtischen Lebensstils, „der ein ganz neues Maß von Reserve und Diskretion erzeugt hat."[56] Simmel fasst zusammen: „Die geschichtliche Entwicklung der Gesellschaft ist in vielen Teilen dadurch bezeichnet, daß früher Offenbares in den Schutz des Geheimnisses tritt, und daß früher Geheimes umgekehrt dieses Schutzes entbehren kann und sich offenbart".[57]

Das Bewahren von Geheimnissen stellt auch für Erving Goffman eine Notwendigkeit zur Produktion und zum Erhalt von Sozialität dar. Üblicherweise arbeiteten alle Akteure an einer gemeinsamen Situationsdefinition mit. Auch die Mitglieder eines Publikums, vor denen soziale Rollen zur Aufführung gebracht werden, kooperierten bei der Bewahrung der Bühnensituation: Sie verhielten sich „diskret" und „taktvoll."[58] Takt und Diskretion bedeuten hier, dass Beobachter keinen Versuch unternehmen, einen Blick in die „back regions" der beobachteten Akteure zu werfen. Würden sie es doch tun, so würden sie Informationen erhalten, die die gemeinsame Situationsdefinition gefährdet, womit die Situation im schlimmsten Falle zusammenbräche.[59] Das Maß an Takt und Diskretion, der Umfang und das Ausmaß des Geheimnisses – von Privatheit also – unterliege dabei kulturhistorischer Variation: „Etiquette regarding tactful inattention, and the effective privacy it provides, varies, of course, from one society and subculture to another."[60] Um zu einer gemeinsamen Situationsdefinition zu gelangen, würden wir also *immer* Front- und Backstage-Bereiche schaffen – *wie* wir das tun, hänge von der kulturhistorischen Situation ab.

Genau einen solchen anthropologischen Universalismus bei gleichzeitigem Kultur-Relativismus vertreten Alan Westin und Irwin Altman. Wie oben angemerkt, betrachtet Westin Privatheit als zoologische Konstante der Evolution: „animals also have minimum needs for private space without which the animal's survival will be jeopardized."[61] Das menschliche Bedürfnis nach Privatheit habe also tierische Wurzeln:

> *„studies of animal behavior and social organization suggest that man's need for privacy may well be rooted in his animal origins, and that men and animals share several basic mechanisms for claiming privacy among their own fellows."*[62]

Dabei könnte es Westin bewenden lassen und schlicht davon ausgehen, dass menschliches Zusammenleben folgerichtig und grundsätzlich ebenfalls immer private Bereiche aufweisen müsse. Stattdessen macht er sich die Mühe,

55 Simmel 1992, S. 401.
56 Simmel 1992, S. 411, 412.
57 Simmel 1992, S. 406.
58 Vgl. Goffman 1973, S. 229.
59 Ein Beispiel dafür wäre das Bezeugen des Streites eines Paares, bei dem man zum Abendessen eingeladen ist. Die Rollen der freundlichen Gastgeber werden von den Informationen gefährdet, die man beim Bezeugen des Streites erhält. Die Gastgeber „fallen aus der Rolle", sie erscheinen als zwei streitsüchtige Individuen, die sich alle möglichen Schwächen vorhalten oder Ähnliches. Dies verträgt sich weder mit der Rolle „nettes Paar" noch mit der Situationsdefinition „harmonisches Abendessen." Im Resultat bricht die Situation zusammen – und die Gäste sind peinlich berührt, weil sie in ihrem Takt und ihrer Diskretion den Blick auf die Hinterbühne ja gar nicht erhaschen wollten.
60 Goffman 1973, S. 230; vgl. auch Ebd., S. 244, 245.
61 Westin 1967, S. 9.
62 Westin 1967, S. 8.

einen Nachweis für diese Universalität zu erbringen, indem er über die Konsultation anthropologischer Wissensbestände die je unterschiedlichen Ausprägungen von Privatheit in den unterschiedlichsten Kulturen analysiert.[63]

Am gleichen Punkt setzt Irwin Altman an:

> *„I hypothesize that all cultures have evolved mechanisms by which members can regulate privacy, but that the particular pattern of mechanisms may differ across cultures."*[64]

Um die Hypothese zu stützen, führt er eine ganze Reihe von Beispielen an. Hier sollen zur Verdeutlichung nur zwei herausgegriffen werden (die sich auch bei Westin finden): Das Erste bezieht sich auf die vergleichenden Untersuchungen, die Clifford Geertz auf Java und Bali durchgeführt hat.[65] Auf Java leben die Menschen demnach in recht offenen Bambushäusern mit dünnen Wänden, die auch von Nicht-Familienmitgliedern nach eigenem Gutdünken betreten werden können. Die mangelnde physische Garantie von Privatheit werde durch Verhaltensregeln aufgefangen: „Javanese shut people out with a wall of Etiquette."[66] Auf Bali lebten die Familien dagegen in Häusern, die von hohen Mauern umgeben seien und die nur von Familienmitgliedern oder engen Freunden betreten werden dürften. Einmal im Haus, sei die Atmosphäre jedoch von „tremendous warmth, humor [and] openness" gekennzeichnet.[67] Das zweite Beispiel bildet das Tragen des Gesichtsschleiers bei den männlichen Tuareg. Diese trügen den Schleier ständig, auch beim Schlafen und Essen, und:

> *„the veil was a literal boundary regulation mechanism and was adjusted and readjusted, however slightly, to reflect openness and closedness to others. Thus, the Tuareg veil serves as an important behavioral mechanism used by people in this culture to control interaction with others [...] these examples illustrate how privacy is a culturally pervasive process."*[68]

Privatheit als individuelles und kollektives Phänomen

Weiter oben wurde schon angemerkt, dass Privatheit als Bestandteil jeder sozialen Beziehung und als sozial konstruiert gelten kann. Darüber hinaus kann sich Privatheit aber nicht nur auf Individuen, sondern auch auf kollektive Gefüge beziehen. Für Simmel ist „jedes Verhältnis zwischen zwei Menschen *oder zwischen zwei Gruppen*" dadurch charakterisiert, „ob und wieviel Geheimnis in ihm ist".[69] Simmel zufolge bestimmt Privatheit damit sowohl die Beziehungen zwischen den Individuen als auch zwischen den Gruppen einer Gesellschaft:

> *„Während das Geheimnis eine soziologische Bestimmtheit ist, die das gegenseitige Verhältnis von Gruppenelementen charakterisiert, oder vielmehr, mit andern Beziehungsformen zusammen dieses Gesamtverhältnis bildet – kann es sich weiterhin mit dem Entstehen ‚geheimer Gesellschaften' auf eine Gruppe als ganze erstrecken."*[70]

Trotz einer recht anderen Argumentation lässt sich mit Erving Goffman derselbe Schluss ziehen. Goffman zufolge kommt es im alltäglichen gesellschaftlichen Rollenspiel nicht nur zur Übernahme und Aufführung individueller Rollen, sondern auch zur Performance ganzer Teams vor

63 Westin 1967, S. 11-18.
64 Altmann 1977, S. 70.
65 Altman 1977, S. 74, 76.
66 Geertz zitiert in Westin 1967, S. 16.
67 Geertz zitiert in Westin 1967, S. 7.
68 Altman 1977, S. 76, 77.
69 Simmel 1992, S. 406 (kursiv d. A.).
70 Simmel 1992, S. 421.

Publikum[71] – so zum Beispiel, wenn Restaurantmitarbeiter vor Kunden arbeiten. Auch in diesen Fällen gäbe es aber immer einen für das Team reservierten Interaktionsbereich, der dem Publikum verborgen bleibe. Alle Aktivitäten, Fakten und Motive, die nicht dem Ideal der Performance entsprechen, würden verborgen oder maskiert.[72] Ein Beispiel hierfür wären rauchende Kellner, die nicht dem Hygieneideal der Gastronomie-Performance entsprechen. Für alle Beziehungen gelte also grundsätzlich:

> *„there is hardly a legitimate everyday vocation or relationship whose performers do not engage in concealed practices which are incompatible with fostered impressions. [...] The larger the number of matters and the larger the number of acting parts which fall within the domain of the role or relationship, the more the likelihood, it would seem, for points of secrecy to exist."*[73]

Während der dem Publikum verborgen bleibende Interaktionsbereich der Teams, die „back region", dabei als kollektive Privatsphäre gelten kann, agieren die Team-Performer als kollektive Geheimniskrämer: „A team, then, has something of the character of a secret society."[74] Individuelle Privatheit lässt sich mit Goffman also als Extremfall denken: Als eine Situation, in der ein einzelner Akteur seine Privatheit gegenüber einem, zwei oder drei Anderen oder gegenüber einer anonymen Masse zu wahren sucht.

Bei Alan Westin folgt indes schon aus der Bestimmung der vier Privatheitsmodi die Existenz kollektiver Privatbereiche. Was Westin als „Intimität" bezeichnet, betrifft beispielsweise ausdrücklich die kollektive Privatheit von zwei oder mehreren Personen.[75] Darüber hinaus bezieht Westin den Privatheitsbegriff auch auf größere kollektive Gefüge, wenn er von einer „Organizational Privacy" spricht.[76] Gemeint ist damit der geschützte Bereich ganzer Organisationen, welchen diese für ihren Selbsterhalt unbedingt bräuchten (um Entscheidungen vorzubereiten können, um über geschützte Kommunikationsräume zu verfügen usw.).

Für Irwin Altman ist zu guter Letzt ohnehin ganz klar:

> *„Privacy can involve different types of **social units**: individuals, families, mixed or homogeneous sex groups, and so on. Sometimes we speak of privacy in terms of one person's blocking off or seeking contact with another person. At other times we can speak of groups' seeking or avoiding contact with other groups or individuals. Thus privacy can involve a great diversity of social relationships – individuals and individuals, individuals and a group, groups and individuals, and so on."*[77]

In der Aufzählung fehlt nur eine Konstellation, die Altman an anderer Stelle dann noch anspricht: „group-to-group social units can be involved."[78] Bei Privatheit handelt es sich also auch insofern um ein soziokulturelles Phänomen, als die involvierten Akteure individuelle wie auch kollektive sein können.

Privatheitsnormen als Ansatzpunkt soziologischer Privatheitsforschung

Alle hier behandelten sozialwissenschaftlichen Klassiker warten mit normativen Privatheitskonzepten auf. Für Simmel gilt Privatheit als „eine der größten Errungenschaften der Menschheit", auch wenn sie nicht *per se* mit „dem Guten"

71 Goffman 1973, S. 77-105.
72 Goffman 1973, S. 43-44 und S. 48.
73 Goffman 1973, S. 64.
74 Goffman 1973, S.104.
75 Westin 1967, S. 31.
76 Westin 1967, S. 42–51.
77 Altman 1975, S. 11.
78 Altman 1975, S. 22.

gleichzusetzen sei;[79] für Goffman ergibt sich der Wert von Privatheit daraus, dass ohne sie die Produktion und der Erhalt von Sozialität schlichtweg unmöglich würden;[80] Westin und Altman weisen Privatheit ausdrücklich positive Funktionen für Individuen und Gesellschaft zu.[81]

Mit Blick auf die zu entwickelnde Forschungsheuristik ist uns an dieser Stelle jedoch die Frage wichtiger, welche soziologische Rolle die Theorien Privatheitsnormen zuweisen. Diesbezüglich ist zunächst festzuhalten, dass sie Privatheit zwar einerseits als durch gesellschaftlich wirksame Normen bestimmt sehen; gleichzeitig gehe Privatheit aber andererseits nicht in solchen Normen auf – zumindest Georg Simmel zufolge nicht:

> *„Wo das zweifellos Unerlaubte so doch unvermeidlich sein kann, ist die Abgrenzung zwischen Erlaubtem und Unerlaubtem um so undeutlicher. Wie weit die Diskretion sich auch der geistigen Antastung ‚alles dessen, was sein ist' zu enthalten hat, wie weit die Interessen des Verkehrs, das Aufeinander-Angewiesensein der Glieder derselben Gruppe diese Diskretionspflicht einschränken – das ist eine Frage, zu deren Beantwortung weder der sittliche Takt noch der Überblick über die objektiven Verhältnisse und ihre Forderungen allein genügt, da vielmehr beides durchaus zusammenwirken muß. Die Feinheit und Komplikation dieser Frage weist sie in viel höherem Grade auf die individuelle, durch keine generelle Norm zu präjudizierende Entscheidung."*[82]

Aus dem Zitat lässt sich zweierlei schließen: Zum einen stehen Privatheitsnormen im Verhältnis zu anderen soziokulturellen Faktoren, das heißt zu anderen Normen, Vorstellungen, Überzeugungen, Leidenschaften, Ängsten usw. Um die Dinge zum anderen noch weiter zu verkomplizieren, stellt Privatheit keinen statischen, durch eine generelle Norm fixierten Bereich dar, sondern wird durch das situative Zusammenwirken verschiedener kollektiver Normen und *individueller* Parameter erzeugt:

> *„Alle diese Momente, die die soziologische Rolle des Geheimnisses bestimmen, sind individueller Natur; aber das Maß, in dem die Anlagen und die Komplikationen der Persönlichkeiten Geheimnisse bilden, hängt zugleich von der sozialen Struktur ab, auf der ihr Leben steht."*[83]

Dieses Ausbalancieren individueller Bedürfnisse und gesellschaftlicher Normen betont auch Alan Westin:

> *„each individual is continually engaged in a personal adjustment process in which he balances the desire for privacy with the desire for disclosure and communication of himself to others, in light of the environmental conditions and social norms set by the society in which he lives. The individual does so in the face of pressures from the curiosity of others and from the processes of surveillance that every society sets in order to enforce its social norms."*[84]

Das Individuum balanciert aber nicht nur Privatheits- mit anderen Normen aus; vielmehr sind gesellschaftliche Normen als abstrakte Orientierungsvorrichtungen zu verstehen, die das Verhalten von Individuen situativ, kontextabhängig und dynamisch formen: „This balance of privacy and disclosure will be powerfully influenced, of course, by both, the society's cultural norms and the particular individual's status and life situation."[85] Eine generelle Beantwortung

79 Simmel 1992, S. 406 und S. 407.
80 Goffman 1973, S. 141.
81 Vgl. Westin 1967, S. 33-37; Altman 1975, S. 45-50.
82 Simmel 1992, S. 399, 400.
83 Simmel 1992, S. 410.
84 Westin 1967, S. 7.
85 Westin 1967, S. 39.

der Frage, wo *die* Privatsphäre beginnt und endet, wäre für Westin und erst recht für Simmel schlichtweg unmöglich, ist doch „Diskretion [...] nach verschiedenen Persönlichkeiten hin verschieden ausgedehnt".[86] Privatheitsnormen kommen demnach immer nur situativ zum Einsatz, wobei eine Aushandlung erfolgt zwischen individuellen Vorstellungen und dem soziokulturellem Kontext, dessen Teil die Privatheitsnormen bilden.

Erzeugt wird dieser Kontext durch eine Reihe von Elementen. Wie oben angemerkt, markieren Individuen und Teams für gewöhnlich Backstage-Bereiche: „The line dividing front and back regions is illustrated everywhere in our society."[87] Das Markieren erfolgt über Zeichen und/oder Materialität: „Given the values of a particular society, it is apparent that the backstage character of certain places is built into them in a material way".[88] Erfolgt eine Invasion in die „back region" trotz materiell-semiotischer Markierung, wirft dies Probleme auf: „I have spoken of the utility of control over backstage and of the dramaturgical trouble that arises when this control cannot be exerted."[89] Gesellschaften weisen private Bereiche aus, und da unterschiedliche Gesellschaften unterschiedliche Werte („values") entwickeln, lassen sich in verschiedenen Gesellschaften eben auch unterschiedliche Privatheitsnormen finden. Diese werden dann auch in nichtmenschliche Dinge materiell (zum Beispiel Architektur) und zeichenhaft (zum Beispiel per schriftlicher Markierung: „do not trespass...") eingeschrieben.

Es gibt mit anderen Worten vielfältige Mittel und Mechanismen zur Erzeugung von Privatheit, wie Irwin Altman erläutert:

> *„People attempt to implement desired levels of privacy by using behavioral mechanisms such as verbal behavior, nonverbal use of the body, environmental behaviors [...] and culturally defined norms and practices."*[90]

Eben diese kulturell (mehr oder minder starr) fixierten Normen bilden die Verhaltensregeln, welche nicht zuletzt die Möglichkeiten der individuellen oder kollektiven Kontrolle persönlicher oder gruppenbezogener Informationen formen: „Rules are at the heart of publicity and privacy. When the rules specify that information is not available to others [...] we can speak of privacy norms."[91] Die Normen der Informationskontrolle bilden in diesem Sinne den Ansatzpunkt soziologischer Privatheitsforschung.

1.2.2 ZUSAMMENFASSUNG UND FOLGERUNGEN

Damit sind fünf zentrale Charakteristika sozialwissenschaftlicher Privatheitsforschung bestimmt. Wir bereits angemerkt, dient die Ausarbeitung dieser nicht dem Zweck der Entwicklung einer umfassenden Privatheitstheorie, und desgleichen ist hier nicht der Ort, an dem eine vollständige Übersicht über sämtliche Überlegungen zum Thema Privatheit in den Sozialwissenschaften geliefert werden soll; die Motive für die Ausweisung der Charakteristika sind vielmehr pragmatischer Natur: Sie stecken das Feld ab, innerhalb dessen wir unsere Forschungsheuristik weiter unten entwickeln werden.

Wir werden dabei zu berücksichtigen haben, dass Privatheit als Kontrolle persönlicher Informationen verstanden werden kann, dass damit aber gleichzeitig der Zugang-zum-Selbst angesprochen ist – eine soziale Beziehung also: „Privacy is not simply a way that information is managed but how social relations are managed."[92] In diesem

86 Simmel 1992,S. 397.
87 Goffman 1973, S. 123.
88 Goffman 1973, S. 124.
89 Goffman 1973, S. 134.
90 Altman 1975, S. 32.
91 Marx / Muschert 2007, S. 382.
92 Dourish / Anderson 2006, S. 327.

Sinne ist Privatheit auch Bestandteil jeder sozialen Beziehung und sozial konstruiert, anthropologisch universal und kulturell relativ, bezieht sich auf Individuen wie auch auf Gruppen. All dieses Charakteristika weisen Privatheit zum einen als Bestandteil einer „Collective Information Practice" und folglich als *soziokulturelles Phänomen* aus: „any adequate account of privacy behaviors, then, must be grounded in an understanding of the specific social and cultural context within which the activity is taking place."[93]

Hinsichtlich der oft thematisierten normativen Dimension von Privatheit nehmen wir zunächst zur Kenntnis, dass Privatheit in der sozialwissenschaftlichen Theoriebildung wie auch in den aktuellen Debatten ein sozialer Wert zugeschrieben wird;[94] gleichzeitig sehen wir unsere Aufgabe nicht in der Entwicklung einer normativ fundierten Privatheitstheorie (dafür sind einige der anderen an diesem Projekt beteiligten Disziplinen besser ausgerüstet). Stattdessen geht es uns darum, die Einsicht sozialwissenschaftlicher Privatheitstheorie aufzunehmen, dass Normen gesellschaftlich produziert werden, gleichzeitig aber immer als Teil eines situativ generierten soziokulturellen Kontextes betrachtet werden müssen. In diesem Sinne sind Normen Elemente eines kontextuellen Geflechtes, das individuell aktualisiert wird. Wie wir dieses Geflecht konzipieren, wird weiter unten erklärt. An dieser Stelle wollen wir mit der Feststellung schließen, dass Privatheitsnormen den Ansatzpunkt soziologischer Forschung bilden.

Damit sind die Umrisse allgemeiner sozialwissenschaftlicher Privatheitstheorie nachgezeichnet. Wir werden die benannten Grundzüge nun als Nächstes vor dem Hintergrund des interdisziplinären Diskurses um soziotechnische Privatheit diskutieren, um so das Feld weiter einzugrenzen, in das sich unsere Heuristik einfügt.

1.3 INTERNET PRIVACY: PRIVATHEIT SOZIOTECHNISCH

Nachdem nun einige Grundzüge sozialwissenschaftlicher Privatheitstheorie geklärt sind, wollen wir diese als Nächstes mit Einsichten bezüglich *soziotechnischer* Privatheit verknüpfen. Der Begriff „soziotechnisch" beschreibt dabei die unhintergehbare empirische Verwobenheit des Sozialen mit dem Technischen: Technische Strukturen werden sozial geformt, Sozialität wird gleichzeitig technisch erzeugt; Technik *ist* sozial, das Soziale *ist* technisch; empirisch sind das Soziale und das Technische letztlich nicht voneinander zu trennen.[95] Auch und gerade für Privatheit gilt, dass diese immer als Teil soziotechnischer Systeme perspektiviert werden muss.[96] Es ist daher kaum verwunderlich, dass mit dem Aufkommen computerisierter Informations- und Kommunikationstechnologien der Status des Privaten regelmäßig als gefährdet eingestuft wurde; spätestens seit den 1960er Jahren beschäftigten sich eine ganze Reihe von Veröffentlichungen mit dem sich wandelnden Status des Privaten, mitunter in Form einer

93 Dourish / Anderson 2006, S. 337. Die Sozialität und Kulturalität von Privatheit sollte aber auch noch aus einem anderen, politischen Grund ernst genommen werden. Wir haben weiter oben bereits darauf hingewiesen, dass Westins Konzipierung von Privatheit am Modell des Individuums vielfach kritisiert wurde, weil Westin Privatheit dadurch als relatives individuelles Recht definiert. Wird Privatheit lediglich als individuelles Recht perspektiviert, tritt es in ein Spannungsverhältnis mit anderen Rechten ein. Priscilla Regan zufolge führt dies dann dazu, dass Privatheit allzu oft gegen konkurrierende Interessen ausgespielt wird (vgl. Regan 1995, S. 15-16). Auf den Punkt gebracht: „If privacy is a right held by an individual against the state, then because no right is absolute, it must be balanced against competing social interests. This leads to a zero-sum game that pits the individual's interest in privacy against society's interest in competing social benefits", so Steeves 2009, S. 193. Allzu leicht kann es dann beispielsweise zu einem „false trade-off between privacy and security" kommen (Solove 2011). Demgegenüber und um dies zu verhindern, betonen Privatheitstheoretiker seit einigen Jahren gebetsmühlenartig den *sozialen* Wert von Privatheit – und zwar gerade angesichts der zunehmenden Verbreitung von Informations- und Kommunikationstechnologien. Vgl. Regan 1995; Introna 1997, Rössler 2001; Solove 2008; Nissenbaum 2010.

94 So etwa Solove 2008, S. 78-100; und Nissenbaum 2010, S. 72-88.

95 Vgl. Bijker / Law 1992.

96 Vgl. Nissenbaum 2010, S. 4-6.

Warnung vor der Zerstörung von Privatheit.[97] Nicht zuletzt bezog auch einer der weiter oben behandelten sozialwissenschaftlichen Klassiker, Alan Westins „Privacy and Freedom", seine Motivation durch das Aufkommen neuer technischer Überwachungsmöglichkeiten.[98]

Die Sensibilität für das soziale Transformationspotenzial neuer Medientechnologien findet sich auch in allen anderen angeführten sozialwissenschaftlichen Klassikern der Privatheitstheorie. So stellt Simmel beispielsweise Überlegungen zu einer „Soziologie des Briefes" an, und zwar

> *„weil der Brief ersichtlich auch von der Kategorie der Geheimhaltung her eine ganz eigenartige Konstellation darbietet. Zunächst hat die Schriftlichkeit ein aller Geheimhaltung entgegengesetztes Wesen. Vor dem allgemeinen Gebrauch der Schrift mußte jede, noch so einfache rechtliche Transaktion vor Zeugen abgeschlossen werden. Die schriftliche Form ersetzt dies, indem sie eine zwar nur potenzielle, aber dafür unbegrenzte ‚Öffentlichkeit' einschließt."*[99]

In ähnlicher Weise erweist sich auch Goffman als Kind seiner Zeit, wenn er den aufkommenden Massenmedien besonderes Augenmerk schenkt:

> *„Another interesting example of backstage difficulties is found in radio and television broadcasting work. In these situations, back region tends to be defined as all places where the camera is not focused at the moment or all places out of range of ‚live' microphones. [...] For technical reasons, then, the walls that broadcasters have to hide behind can be very treacherous, tending to fall at the flick of a switch or a turn of the camera."*[100]

Während Alan Westins Fokus auf neue Überwachungstechnologien schon angesprochen wurde, stellte Irwin Altman jedenfalls in Rechnung, dass die verschiedensten Mechanismen zur Erzeugung (und also auch Zerstörung) von Privatheit herangezogen werden könnten.[101] Altman lässt sich dabei ohne Weiteres so verstehen, dass zu diesen Mechanismen auch technische gehören.

In allen Fällen ermöglichen neue Technologien einen neuartigen Umgang mit Informationen und damit gleichzeitig auch die Schaffung neuartiger sozialer Situationen. Die Angemessenheit unseres doppelten Privatheitsverständnisses als Informationskontrolle und Zugang-zum-Selbst ergibt sich aber nicht aus den soziotechnischen Situationen, die die Klassiker thematisieren; auch aktuelle Forschungen zu Internet-bezogenen Phänomenen bestimmen Privatheit auf diese Weise. danah boyd leitet aus ihrer Untersuchung von *Social Network Sites* zum Beispiel Folgendes ab:

> *„Privacy is a sense of control over information, the context where sharing takes place, and the audience who can gain access. Information is not private because no one knows; it is private because the knowing is limited and controlled."*[102]

Zwar kritisiert Solove die Definition von Privatheit-als-Kontrolle-persönlicher-Informationen als „too vague, too broad, or too narrow",[103] weil beispielsweise weder klar wäre, was Kontrolle, noch was „persönlich" genau meine;[104] jedoch besteht Soloves Interesse in einer Klärung

97 Vgl. dazu Solove 2008, S. 4.
98 Westin 1967, S. 3.
99 Simmel 1992, S. 429.
100 Goffman 1973, S. 119.
101 Altman 1975, S. 32-42.
102 boyd 2008, S. 18.
103 Solove 2008, S. 29.
104 Solove 2008, S. 25, 26 und 28.

des Privatheitskonzeptes für die Rechtswissenschaften und -sprechung. Und: „Legal protections of privacy depend upon a conception of privacy that informs what matters are protected and the nature and scope of the particular protections employed".[105] Die Rechtsprechung erfordert mit anderen Worten eine klare, möglichst umfassende und eindeutige Definition von Privatheit frei von Ambiguitäten. Für die empirische soziologische Erforschung des Phänomens *Internet Privacy* ist eine solche umfassende Definition jedoch nicht erforderlich, weil dabei erstens ein begrenztes Praxisfeld untersucht wird (eben ***Internet Privacy***), und weil die Frage, was „Kontrolle" oder „persönlich" genau heißen mag, *empirisch gewendet* wird: Für die Antworten hierauf sind die befragten Akteure verantwortlich.

Darüber hinaus ist es auch kaum verwunderlich, dass sich hinsichtlich der Taxonomie, die Solove zur Markierung von Privatheitsproblemen vorschlägt, drei der vier angegebenen Praxistypen auf Informationen beziehen: die Sammlung, die Übertragung und die Verbreitung von Informationen.[106] Mit Bezug auf die bisherigen Feststellungen können wir also davon ausgehen, dass das Sammeln, Übertragen und Verbreiten von Informationen von soziotechnischen Situationen geformt wird und seinerseits solche Situationen formt. Die Praktiken des Sammelns, Übertragens und Verbreitens erfolgen mit anderen Worten vor dem Hintergrund eines sozial-kulturell-technischen Kontextes,[107] welcher Normen enthält.[108] Aus dem Zusammenspiel dieser Faktoren ergibt sich schließlich die „Collective Information Practice" der Erzeugung soziotechnischer Privatheit.[109]

Daraus ergeben sich drei Folgerungen für die Heuristik:

a) Ausgangspunkt der Entwicklung der Heuristik sollte eine robuste Konzipierung der Praktiken der Internetnutzung sein, denn: „Privacy is not a concept that can be separated from the collective practices through which it is achieved and made operable or from the other elements that are achieved through those same practices."[110] Das Praxiskonzept sollte zudem in Rechnung stellen, dass wir es bei der Nutzung des Internets mit *soziotechnischen* Praktiken zu tun haben.

b) Insofern die Praxis der Internetnutzung vor dem Hintergrund eines (teilweise technisch erzeugten) soziokulturellen Kontextes stattfindet, muss Privatheit-als-Informationskontrolle mit Praxis, Sozialität, Kultur und Technologie zusammen gedacht werden,[111] wobei die genannten Faktoren allerdings (zumindest analytisch) unterscheidbar bleiben müssen.

c) Die Heuristik muss in der Lage sein, Privatheitsnormen einen angemessenen Platz einzuräumen. „Angemessen" meint, dass Normen als Teil des soziokulturellen Kontextes konzipiert werden und auf informationelle Praktiken zu beziehen sein müssen; sie müssen darüber hinaus als nicht-determinierend, aber Praxis-formend und als meta-stabil zu denken sein. Es ist davon auszugehen, dass neue Technologien bis dato gültige Normen und Werte einerseits reproduzieren können; andererseits kann auch genau das Gegenteil der Fall sein: „[Information and Communication Technologies] can indeed be constitutive of new social dynamics, but they can also be derivative or merely reproduce older conditions."[112] Beiden Möglichkeiten muss die Heuristik Rechnung tragen können.

Zu dieser kommen wir nun.

---

105 Solove 2008, S. 4.
106 Vgl. Solove 2008, S. 101-161.
107 Dourish / Anderson 2006, S. 337.
108 Nissenbaum 2010, S. 137-147; Solove 2008, S. 41.
109 Dourish / Anderson 2006.
110 Dourish / Anderson 2006, S. 338.
111 Solove 2008, S. 50.
112 Sassen 2004, S. 365.

1.4 ENTWURF DER FORSCHUNGSHEURISTIK

Im Folgenden stellen wir unsere Forschungsheuristik vor. „Heuristik" meint hier ein abstraktes Begriffsinstrumentarium, das es uns erlaubt, empirische Fragen zu stellen und die gegebenen Antworten zu analysieren. Es geht uns also nicht darum, eine allgemeingültige Privatheitstheorie zu entwickeln, die jeder möglichen ontologischen Artikulation von Privatheit Rechnung trägt, sondern darum, eine begrifflich spezifizierte und empirisch operationalisierbare Fragestellung zu entwickeln. Da Privatheit (wie oben ausgeführt) aus soziotechnischer Perspektive als „Collective Information Practice" zu konzipieren ist,[113] setzen wir zunächst mit der Frage an: *Was genau verstehen wir unter dem Ausdruck „Praxis der Internetnutzung?"*

1.4.1 OPERATIONSKETTEN

Unseren Ausgangspunkt bildet hier eine in der französischen Technikanthropologie entwickelte[114] und in den *science and technology studies* aufgenommene[115] Grundkategorie: Die Operationskette. Wenn ein menschlicher Akteur einen Computer nutzt, so verstehen wir dies als die Erzeugung einer Operationskette mit menschlichen und technischen Anteilen. Die Operationen der Nutzer bestehen darin, wahrzunehmen, zu denken, zu fühlen, Interessen zu entwickeln usw. Die Nutzer nehmen die Oberfläche des Computers wahr (Interface) und manipulieren diese (über die Maus, die Tastatur etc.), woraufhin der Computer weitere Operationen ausführt (binär-digitale Rechenvorgänge). Im Resultat entsteht eine operative Gesamtkette oder Operationskette – welche an Komplexität zunimmt, wenn der genutzte Computer an das Internet angeschlossen ist.

1.4.2 KULTUR-PROGRAMME

Wie aber unterscheiden wir die Praxis der Internetnutzung von beliebigem oder zufälligem Umgang mit Informations- und Kommunikationstechnologien (IKT)? Stichhaltig kann ja von Praxis nur dann die Rede sein, wenn die Internetnutzung bestimmte stabile Muster aufweist. Was trägt die Verantwortung für diese Stabilisierung der Nutzungsprozesse und die daraus resultierende Erkennbarkeit von Nutzungsmustern? Unserem heuristischen Rahmen zufolge sind diesbezüglich *Programme* zu nennen.[116] Diese operieren einerseits aufseiten der menschlichen Nutzer; es handelt sich um *kognitive* Skripte, welche in Form impliziten und expliziten Wissens vorliegen.[117] Empirisch können diese als Nutzendefinitionen, Wahrnehmungsraster, Bedeutungsgewebe, Anwendungswissen – und eben als Nutzungsnormen auftreten. *In all diesen Dimensionen kommt implizites oder explizites Wissen zum Zuge, welches den menschlichen Anteilen der Operationskette Form verleiht.* Bei der Nutzung eines Computers formt die Vorstellung vom Nutzen der Aktivität genauso die von Menschen ausgeführten Operationen, wie die kulturspezifische Art und Weise der Wahrnehmung, die der Wahrnehmung zugewiesene Bedeutung, der Kompetenzgrad der Nutzer (Anwendungswissen) und die kulturelle Definition akzeptablen Verhaltens (Normen). Um ein plakatives Beispiel anzubringen: In China ist es üblich, die Farbe Rot mit Glück zu assoziieren, in Europa dagegen mit Gefahr. Es ist leicht nachzuvollziehen, dass diese kulturell bestimmte Art und Weise der Wahrnehmung und Bedeutungszuweisung das Nutzungsverhalten prägt.

Auch die technischen Sequenzen der Computernutzung werden über Programmanteile geformt, über *technische* Skripte.[118] Diese verleihen den Operationen der Apparate Stabilität, machen sie kalkulierbar und an die Operationen

113 Dourish / Anderson 2006.
114 Vgl. Leroi-Gourhan 1987.
115 Vgl. Akrich 1992; Latour 1992.
116 Leroi-Gourhan 1987, S. 288-295.
117 Bauer 2006.
118 Akrich 1992; Latour 1992.

der menschlichen Nutzer anschließbar. Solchermaßen kann eine relativ stabile Operationskette entstehen, welche Einzeloperationen menschlicher Akteure und technischer Komponenten enthält. Beide Programmanteile – sowohl die kognitiven als auch die technischen Skripte – werden kulturell (nicht-genetisch) weitergegeben. Bei den menschlichen Anteilen kann dies unbewusst (zum Beispiel über Spiegelneurone, per Nachahmung) oder bewusst (zum Beispiel über Unterricht, per Unterweisung) erfolgen; die technischen Skripte werden indes in Dokumente (zum Beispiel technische Zeichnungen) und Apparate (zum Beispiel Software) zeichenhaft und materiell eingeschrieben und überliefert. *Es handelt sich bei Programmen daher um Kultur.*

Teil dieser Kultur sind spezifische Verhaltensregeln, an denen sich die Akteure orientieren –Normen: „Behavior guiding norms prescribe and proscribe acceptable actions and practices."[119] Ein solches Verständnis von Normen als Vor-schrift („pre-scription") ist mit dem Konzept des Kultur-Programms vollkommen vereinbar, wie die Etymologie des Programm-Begriffs verdeutlicht: Der Terminus kommt vom griechischen *prógramma* und meint eben etwas „Vorgeschriebenes" oder eine „Vorschrift." Insofern Programme, und das heißt auch Normen, die Operationsketten formen, die wir als „Praxis" bezeichnen, lassen sich aus der Analyse von Kultur-Programmen Praktiken rekonstruieren. Wie weiter oben angemerkt, ist dabei zu berücksichtigen, dass Praktiken keine triviale Exekution vorgehender Programmstrukturen darstellen, sondern eine dynamische Aktualisierung von Kultur-Programmen. Letztere sind in diesem Sinne meta-stabil, sie sorgen für relative Stabilität; jede Aktualisierung eines Kultur-Programms ist indes kreativ, bietet die Möglichkeit der Veränderung. Kultur wird in diesem Sinne in jedem Moment neu erfunden, allerdings vor dem Hintergrund bis dato bestehender Kultur. Zudem orientieren sich Akteure an Programmen und führen sie nicht bloß aus. Das Kultur-Programm, das das Sitzen auf Stühlen festlegt, ist von prekärer Stabilität; zuweilen stehen Akteure auf Stühlen oder tanzen auf Tischen. Das Einschreiben von Programmanteilen in Dinge (Artefakte, Dokumente) ermöglicht aus techniksoziologischer Sicht eine Stabilität, die menschlichen Sozialformationen eigen ist.[120] Werden zum Beispiel Normen in Artefakte eingelassen, dann werden auf diese Weise (technische) Anteile von Operationsketten stabilisiert, weil die Artefakte selbst ihre Skripte nicht kreativ verändern. In diesem Sinne *stabilisiert* Technologie Gesellschaft. Beispielsweise wird die Verhaltensregel, nur angeschnallt Auto zu fahren, materiell und zeichenhaft implementiert, indem zunächst Anschnallgurte erfunden werden, die es den Fahrern ermöglichen, trotz des Gurtes das Gefährt zu steuern (die Bewegungsfreiheit wird nicht eingeschränkt, der Gurt blockiert nur beim Aufprall). In vielen Autos ertönt zudem ein unangenehmes Alarmsignal (Zeichen), wenn die Fahrer unangeschnallt losfahren. Die Norm wird materiell-semiotisch in das Artefakt eingeschrieben.[121] Solche Einschreibungen erfolgen bereits beim Design technischer Artefakte.[122]

Normen sind solchermaßen als Elemente eines soziokulturellen Kontextes zu verstehen: Sie sind Teil eines dynamischen Kultur-Programms, das zwar für eine gewisse Stabilität sorgt, situativ immer wieder neu erfunden wird. Mit der Einführung neuer Technologien treten neuartige Operationsweisen auf, die mit den Operationen der Nutzer verknüpft werden. Dabei wird bislang existierenden normativen Erwartungen der Nutzer entsprochen – diese werden also reproduziert – oder die Normen der Nutzer passen sich an die neuartigen Operationsweisen an. Nutzungsnormen werden folglich reproduziert, modifiziert, neu erfunden.[123] Da Kultur-Programme und deren normative Elemente als dynamisch zu konzipieren sind, kann Wandel indes *mit jedem Vollzug* des Kultur-Programms auftreten. Auch die

119 Nissenbaum 2010, S. 133.
120 Vgl. Strum / Latour 1987.
121 Das Beispiel stammt aus Latour 1992.
122 Vgl. Flanagan / Howe / Nissenbaum 2008.
123 Marx 1994.

resultierenden Praktiken sind dann meta-stabil. Für Informations- und Kommunikationstechnologien heißt das: „information technology does not simply encode social practice but is a site at which it is developed."[124] In diesem Sinne betrachten wir „information systems as sites for the production of social and cultural values."[125] Die Einführung neuer Technologien ruft also eine Doppelbewegung hervor: Das Einschreiben bis dato existenter Normen in die soziotechnischen Systeme und/oder die technisch hervorgerufene Transformation bislang bestehender Normen.

Auf eben diese Weise verstehen wir die in der Projektüberschrift angeführte „Kultur der Privatheit und des Vertrauens." Nachdem nun die grundsätzliche Terminologie unserer Heuristik geklärt ist, muss als Nächstes noch erläutert werden, wie Privatheit und Vertrauen unter Bezug auf die Heuristik zu konzipieren sind. Eben dazu kommen wir nun.

1.4.3 PRIVATHEIT ALS KONTROLLIERTE VERKNÜPFUNG VON OPERATIONSKETTEN

Wie in Kapitel 1.2 festgestellt, sollte Privatheit als soziokulturelles Phänomen verstanden werden; wenn wir in unserer Heuristik Privatheit-als-Informationskontrolle fassen, so ist es zudem geboten, von einer Vorstellung kollektiver Informationspraxis auszugehen, welche ihrerseits Sozialität und Kultur zu unterscheiden erlaubt und Normen einen angemessenen Platz einräumt. Wie zu sehen war, sind wir bei unserer Konzipierung der Heuristik in der Tat von der Praxis der Internetnutzung ausgegangen; die Konzipierung von Kultur als Programm erbrachte ein dynamisches Kontextverständnis, wobei Normen als Elemente dieses dynamischen kontextuellen Geflechtes verstanden worden sind. Im nächsten Schritt wollen wir nun die Heuristik mit dem Privatheitskonzept verknüpfen: Was meint Privatheit aus Sicht der Heuristik und unter Berücksichtigung der Annahme, dass „privacy and security rather as social products than natural facts" zu betrachten sind?[126]

Techniksoziologisch – das heißt hier vom Konzept der Operationskette her gedacht – lässt sich Sozialität (der Aufbau von Beziehungen) als eine *Verknüpfung von Operationsketten* verstehen. Im Zuge angesichtiger Interaktion verknüpfen sich beispielsweise die Operationen eines Akteurs (zum Beispiel sprachliche Äußerungen) mit denen eines anderen Akteurs (Wahrnehmung von Körperhaltung, Lauten usw.); über die Interaktion bildet sich eine Beziehung. Davon zu unterscheiden wäre dann (wie oben ausgeführt) Kultur als *Formung* von Operationsketten (*wie* gesprochen wird, wie sich die Körper zueinander verhalten, wie das alles wahrgenommen wird, ist kulturell bestimmt). Im Falle von Interaktivität, das heißt von nicht-angesichtiger Interaktion, gewinnt die Verknüpfung von Operationsketten dann einiges an Komplexität.

Aus einer solchen Perspektive handelt es sich bei Privatheit um die Möglichkeit von Nutzern, Operationsketten zu verknüpfen, ohne deshalb die Kontrolle über die Informationen zu verlieren, welche über die so gebildete Beziehung vermittelt werden.[127] Privatheit meint also auch im Rahmen unserer Heuristik immer die Privatheit-*in*-Beziehungen. Nutzen Akteure etwa *Social Network Sites*, dann knüpfen sie Beziehungen; entzieht sich die über diese Beziehungen erfolgende Verbreitung von Informationen der Kontrolle der Akteure, so verlieren diese damit die Möglichkeit, den Grad an Privatheit zu regulieren, den sie als angemessen erachten. Die normativen Anteile ihres Kultur-Programms (ihre

124 Dourish / Anderson 2006, S. 335.
125 Dourish / Anderson 2006, S. 332.
126 Dourish / Anderson 2006, S. 335, 336.
127 Wir bestimmen an diesem Punkt nicht, was „Kontrolle" und „persönliche Information" genau meint, sondern überlassen diese Bestimmung den Nutzern. Aus diesem Grunde reden wir hinsichtlich unseres theoretischen Rahmens nicht von einer „Theorie", sondern bescheidener von einer „Forschungsheuristik."

Privatheitsnormen) können dann in Widerspruch zum technischen Anteil des Kultur-Programms (die Software der SNS) geraten. Die Qualität der geknüpften Beziehungen (welche vom Kultur-Programm bestimmt wird) kommt schließlich mit den Erwartungen der Nutzer in Konflikt, Letztere verlieren die Möglichkeit, das für die Beziehung angemessene Maß an Privatheit erzeugen.

An diesem Beispiel deutet sich schon an, das in Bezug auf *Internet Privacy* vor allem „context-relative informational norms"[128] als Teile jener Kultur-Programme zu berücksichtigen sind, die die Praktiken regulieren. In diesem Sinne regulieren

> *„informational norms [...] the flow of information of certain types about an information subject from one actor (acting in a particular capacity, or role) to another or others (acting in a particular capacity or role) according to particular transmission principles."*[129]

Und wie immer bei der Einführung neuartiger Technologien (technischer Operationsweisen) ist auch in Bezug auf die Privatheitsnormen informationeller Praktiken davon auszugehen, dass die Technologien als Auslöser von Normenwandel fungieren (können):

> *„The technical changes in surveillance and communications means have brought great challenges to contemporary norms of information control. With the advent of computerization and other information related tools, these fundamental changes are altering norms and related social forms that govern social life."*[130]

Ein Beispiel dafür wäre das Telefonieren in der Öffentlichkeit. Während Telefonzellen als geschützte Privatbereiche im öffentlichen Raum gelten,[131] führen viele Menschen mittlerweile über ihr Handy Privatgespräche in der U-Bahn, im Bus usw. Im Juli 2011 veröffentlichte die österreichische Marktforschungsfirma Spectra die Ergebnisse einer repräsentativen Umfrage zum Thema Handy-Nutzung in der Öffentlichkeit und kam zu folgendem Ergebnis: „Insgesamt kann man davon ausgehen, dass sich mehr als jeder zweite Österreicher (58 %) zumindest manchmal vom Telefonieren in der Öffentlichkeit gestört fühlt."[132] Besonders interessant ist jedoch folgende Beobachtung: „Uneingeschränktes Mobiltelefonieren in der Öffentlichkeit korreliert sehr stark mit dem Alter. Während sich jeder zweite Mobiltelefonbesitzer unter 30 Jahre beim Telefonieren nicht um seine Umgebung kümmert, macht dieser Anteil in der Generation 50+ nur 22 % aus."[133] Hier liegt der Gedanke nahe, dass jüngere Nutzer die Unterscheidung Öffentlichkeit / Privatheit auf andere Art und Weise einsetzen, als die älteren – dass sich hier *die (Privatheits-)Normen der jüngeren Nutzer an die neuartigen Operationsmöglichkeiten (Mobiltelefonie) angepasst haben*; und dass sich die älteren Nutzer deshalb gestört fühlen, weil sie dahingegen verlangen, dass *bislang bestehende Normen in der Nutzungskultur für Mobiltelefone reproduziert werden.*

Das Beispiel verdeutlicht weiter, dass Privatheitsnormen in der Tat als Teil eines dynamischen, wandelbaren soziokulturellen Kontextes gelten müssen. Mitunter weisen verschiedene Gruppen unterschiedliche Normen auf. Letztere stehen als Elemente von Kultur-Programmen zudem immer in – zum Teil widersprüchlicher – Beziehung zu anderen Elementen des Kultur-Programms. Sie können folglich nur im Zusammenhang mit diesen anderen Elementen analysiert werden,[134] das heißt im Zusammenhang mit kulturell geprägten Vorstellungen, Überzeugungen, Normen, Glaubenssätzen, Wünschen und Befürchtungen sowie soziokulturellen Definitionen von

128 Nissenbaum 2010, S. 137-147.
129 Nissenbaum 2010, S. 141.
130 Marx / Muschert 2009, S. 229. Vgl. auch boyd 2008, S. 14; Flanagan / Howe / Nissenbaum 2008, S. 327.
131 Nissenbaum 2010, S. 115.
132 Spectra 2011, S. 1.
133 Spectra 2011, S. 1.
134 Nissenbaum 2010, S. 139-140.

Gefahr, Risiko, Sicherheit, ökonomischen Vorteil.[135] Die Frage nach den Normen bildet also für die sozialwissenschaftliche Privatheitsforschung den *Ansatz*- im Sinne eines *Ausgangs*punktes. Von dort aus erfolgt der Zuschnitt der Fragestellung und des Forschungsdesigns, und von dort aus werden weitergehende Erkenntnisse zur Thematik generiert.

Wie aber ist nun nach den Privatheitsnormen zu fragen? Für eine kontextbezogene Bestimmung von Privatheit hat es sich als furchtbare Strategie erwiesen, essentialistische Definitionen fallen zu lassen und stattdessen Privatheits*probleme* zu identifizieren und zu klassifizieren.[136] Für Privatheitsnormen heißt das: Sie werden dann sichtbar, wenn Nutzer angeben, in ihrer Privatheit *verletzt* worden zu sein. Erkenntnisse darüber, wie Privatheit von den Nutzern bestimmt wird, lassen sich also gewinnen, indem wir nach Verletzungen ihrer Privatheit fragen.

Für den sozialwissenschaftlichen Anteil des Projektes geht die generelle Stoßrichtung der Forschung folglich in Richtung der Frage, ob die Nutzer im Internet über ausreichende Möglichkeiten verfügen, bei der Verknüpfung von Operationsketten ihre Informationen zu kontrollieren, um auf diese Weise Privatheit zu erzeugen und Vertrauen in die Technologie aufzubauen. Damit kommen wir zum letzten zu klärenden Begriff, dem des Vertrauens.

1.4.4 VERTRAUEN INS NICHT-MENSCHLICHE GEGENÜBER

Bezüglich des Vertrauens lässt sich zunächst eine gewisse Einigkeit verschiedener soziologischer Forschungs- und Theorieansätze konstatieren, sofern dessen wichtige Rolle gegenüber sozialer Komplexität betroffen ist.[137] Schon für Georg Simmel war das Vertrauen – „eine der wichtigsten synthetischen Kräfte innerhalb der Gesellschaft" und „mittlerer Zustand zwischen Wissen und Nichtwissen" – unerlässliche Voraussetzung für die Produktion sozialer Beziehungen, und zwar gerade, weil solche Beziehungen notwendig und grundsätzlich ein Mindestmaß an Privatheit aufweisen.[138] Mit dem Eintritt in die Moderne werde Vertrauen zudem für die Erzeugung von Sozialität immer wichtiger, denn in der Moderne stünde

> *„das Leben auf tausend Voraussetzungen, die der einzelne überhaupt nicht bis zu ihrem Grunde verfolgen und verifizieren kann, sondern die er auf Treu und Glauben hinnehmen muß. In viel weiterem Umfange, als man sich klar zu machen pflegt, ruht unsre moderne Existenz [...] auf dem Glauben an die Ehrlichkeit des andern. Wir bauen unsere wichtigsten Entschlüsse auf ein kompliziertes System von Vorstellungen, deren Mehrzahl das Vertrauen, daß wir nicht betrogen sind, voraussetzt."*[139]

In der Techniksoziologie werden recht ähnliche Debatten unter dem Stichwort einer „Sozialität mit Objekten" geführt,[140] um den Umstand zu betonen, dass Beziehungen aktuell in immer stärkerem Maße ohne ein klar identifizierbares, individuelles und menschliches Gegenüber gebildet werden. Im Rahmen der hier vorgeschlagenen Heuristik lässt sich eine solche Sozialität mit Objekten als eine Verknüpfung von Operationsketten mit apparativen Vorrichtungen und abstrakten Strukturen verstehen. Zwar gehen die Nutzer üblicherweise davon aus, dass die

135 Vgl. dazu Dourish / Anderson 2006, S. 338.
136 Solove 2008, S. 10 und S. 101-170.
137 So spricht Niklas Luhmann von „Systemvertrauen" und hebt damit auf das Handeln unter der Bedingung der Unkenntnis von Handlungspartnern (und deren Handlungen) ab, vgl. Luhmann 2000. In ähnlicher Weise versteht Anthony Giddens Vertrauen als Voraussetzung für das Funktionieren abstrakter Expertensysteme, vgl. Giddens 1995.
138 Simmel 1992, S. 393.
139 Simmel 1992, S. 388, 389.
140 Knorr-Cetina 1998.

mit den Apparaturen gebildeten Operationsketten sich früher oder später wieder mit menschlichen Operationen verknüpfen,[141] doch lässt sich die Verantwortung für die Wahrung kommunikationsregulierender Normen nicht mehr allein auf ein direktanwesendes Gegenüber zurechnen: „People, including the younger generation, still care about privacy. [...] They're not technically sophisticated about privacy and make mistakes all the time, but that's mostly the fault of companies and Web sites that try to manipulate them for financial gain."[142] Aus diesem Grunde sollten sich nicht nur die *Transmissionsprinzipien* der Apparaturen in Übereinstimmung mit den Normen der Nutzer zur Regulierung des Informationsflusses befinden, sondern soll Vertrauen erzeugt werden, müssen die abstrakten Systeme zudem auch Transparenz und Rückmeldungen für die Nutzer bereithalten, Garantien, dass ihre Normen auch dann gewahrt bleiben, wenn es in der Interaktion kein eindeutig verantwortlich zu machendes menschliches Gegenüber gibt. „Vertrauen" bedeutet in diesem Sinne, dass die technischen Skripte so gestaltet sind, dass die Nutzer ihnen ihre Normen zur Informationsregulierung einschreiben können, und dass die Nutzer auch einen Nachweis erhalten, dass dies tatsächlich erfolgt. Der Begriff der „Informationsregulierung" bezieht sich dabei sowohl auf die Verknüpfung wie auch auf die Formung von Operationsketten: Die Nutzer müssen zum einen kontrollieren können, *wer Zugang* zu ihren Informationen in einem einzelnen Interaktivitätsakt erhält, und in welchen Datenbanken ihre Daten landen – mit welchen Ketten sich ihre eigenen Operationen also nach der Ursprungsinteraktivität verknüpfen. Zum anderen müssen die Nutzer auch kontrollieren können, *zu welchen ihrer Informationen* andere Akteure Zugang haben, und welche ihrer Informationen in Datenbanken oder anderswo landen.

1.4.5 ABLEITUNG DER FORSCHUNGSFRAGE

Hier wird es uns nun abschließend um die wichtige Aufgabe gehen, die Grundzüge unserer Heuristik in die Frage nach *Internet Privacy* zu überführen. Sehr allgemein gesprochen, geht es dabei darum, empirisch zu untersuchen, ob die Nutzer im Internet über ausreichende Möglichkeiten verfügen, Privatheit zu erzeugen. In der Terminologie unserer Heuristik mündet dies in folgende Fragestellung:

Welche Privatheitsnormen sind Anteile der Kultur(-programme) der Nutzer, halten sie diese für in ausreichender und angemessener Weise in die Technologien eingeschrieben, und enthalten die soziotechnischen Systeme nachvollziehbare Rückmeldungs- und Transparenzmechanismen zum Aufbau von Vertrauen?

In der Fragestellung implizit enthalten sind zudem Fragen danach, mit welchen sonstigen Elementen des Kultur-Programms die Privatheitsnormen der Nutzer in Beziehung und Widerspruch stehen, ob und (wenn ja:) welche Privatheitsverletzungen die Technologien hervorrufen und inwieweit die Normen einem technologisch-induzierten Wandel unterliegen beziehungsweise bereits unterlegen sind. Wie in der qualitativen Sozialforschung üblich, dient uns die Frage als Ausgangspunkt der Untersuchung, der den Zuschnitt des Forschungsdesigns anleitet. Von der Untersuchung selbst erhoffen wir uns gleichwohl nicht-antizipierte Erkenntnisse. Wir testen also keine Hypothesen, sondern wählen einen Mittelweg zwischen radikal theoriegenerierenden und radikal theoriegeleiteten Forschungsansätzen: Die theoriegeleitete Formulierung der Fragestellung soll die Generierung neuer (theoretischer oder zumindest theoretisierbarer) Erkenntnisse ermöglichen.

[141] Die meisten Nutzer versenden beispielsweise E-Mails, weil sie davon ausgehen, dass diese – nachdem die Daten über eine ganze Reihe von Maschinen gelaufen sind – schließlich wieder von anderen Nutzern gelesen werden.

[142] Schneier 2010.

Im nächsten Schritt werden wir die Fragestellung nun im Zuge der Entwicklung des Forschungsdesigns empirisch operationalisieren.

1.5 DAS FORSCHUNGSDESIGN

Ziel der Forschung ist es, Erkenntnisse darüber zu gewinnen, wie Privatheit von verschiedenen Nutzergruppen definiert wird. Zudem geht es darum, benachbarte Faktoren, wie Einschätzungen von Risiko und Gefahr, Befürchtungen und Wünsche von Nutzern zu identifizieren. Im Folgenden erörtern wir die Konstruktion des Forschungsfeldes und die zum Einsatz gebrachte Methode, um dann schließlich die konkrete Durchführung zu erläutern.

1.5.1 KONSTRUKTION DES FORSCHUNGSFELDES

Insbesondere in Deutschland haben Nutzer in die Sicherheit des Internets wenig Vertrauen. In einer Befragung von 5.030 deutschsprachigen Bürgern (repräsentativer Querschnitt) geben 60 Prozent der Befragten an, dass sie starke Zweifel an der Sicherheit des Internet haben.[143] Insbesondere befürchten sie die Überwachung beziehungsweise Ausspähung der eigenen Privatsphäre. Drei Viertel aller Deutschen sind der Auffassung, dass sie keine vollständige Kontrolle über ihre persönlichen Daten haben. Dabei zeigt sich, dass Bildung, Geschlecht und Einkommen wenig Einfluss auf die Stärke des Sich-Sorgen-Machens haben, nur Alter wirkt sich in der Weise aus, dass mit dem Älterwerden auch das Misstrauen leicht ansteigt. Viele Bürger (ebenfalls 60 Prozent der Befragten) äußern, dass sie ein „ungutes Gefühl" angesichts der Entwicklungen haben. Dieses „ungute Gefühl" wird bislang jedoch ebenso wenig wie die Befürchtung vor Überwachung inhaltlich genau bestimmt. Weitere Studien kommen zu dem Ergebnis, dass (deutsche) Bürger vor allem fehlendes Vertrauen an die Sorge um den Verlust von Privatheit knüpfen,[144] wobei sie Privatheit im Kontext des Internet als Recht fassen, die eigenen Daten kontrollieren zu können.[145] Studien aus dem amerikanischen Raum weisen indes *privacy policies* für amerikanische Nutzer wenig Bedeutung zu, sofern es darum geht, dass diese Vertrauen ins Internet entwickeln.[146] Auffallend ist auch die Erkenntnis, dass Web 2.0-affine Nutzer eine höhere Bereitschaft haben, private Informationen zu veröffentlichen als technikdistanziertere Nutzer.[147] Allerdings bedeutet dies nicht, dass sie nicht die gleichen Wünsche an Sicherheit haben, es heißt nur, dass technikaffine Nutzer risikobereiter sind. Den Wunsch nach Schutz und die Sorge vor Missbrauch teilen beide Gruppen.

Angelehnt an diese Befunde, unterscheiden wir zunächst die beiden Gruppen der technikaffinen und der technikdistanzierten Internetnutzer und setzen mit der Arbeitshypothese an, dass diese beiden Gruppen nicht die gleichen Privatheitsvorstellungen aufweisen und sich ebenso wenig die gleichen Sorgen hinsichtlich der Umsetzung dieser in technischen Anwendungen machen. Ins Zentrum der Analyse rücken wir die technikaffinen Nutzer, weil diese eine höhere Risikobereitschaft aufweisen, dabei gleichzeitig keine geringere Skepsis gegenüber der IT-Sicherheit haben. Es ist davon auszugehen, dass diese Gruppe zudem hohen Einfluss auf die Meinungsbildung in der Gesellschaft hat. Zusätzlich differenzieren wir die Gruppe der technikaffinen noch nach Alter: in eine Gruppe, deren Mitglieder eine Welt ohne Internet nicht mehr kennengelernt haben, und eine Gruppe von technikaffinen Nutzern, bei denen dies nicht der Fall ist. Solchermaßen kann ein möglicher Normenwandel kenntlich gemacht werden. Die technikdistanzierten Nutzer werden als Kontrollgruppe befragt.

143 S. Dörflinger 2009.
144 So etwa Dörflinger 2009, aber auch die Arbeiten von Hodel/Schütte/Biedermann 2008.
145 So auch Dörflinger 2009.
146 Vgl. Sultan / Urban / Shankar / Bart 2002.
147 Vgl. Reinecke / Trepte 2008.

Zu guter Letzt unterscheiden wir noch eine vierte Gruppe: professionelle Experten, wie etwa IT-Sicherheitsspezialisten und Datenschutzbeauftragte. Diese dürften zum einen den Sicherheits- und Privatheitsdiskurs besonders gut kennen; zum anderen sind sie alltäglich mit den Problemlagen technischer und rechtlicher Infrastrukturen vertraut. Unterscheidet sich die Problemidentifizierung der Experten von denen der Nutzer, so lassen sich daraus wertvolle Erkenntnisse gewinnen. Zusammengefasst unterteilen wir das Feld nach folgenden Gruppen:

- *Digital Natives* (18-25 Jahre alte internetbegeisterte Menschen);
- *Technikaffine Bürger* (über 25 Jahre, technikbegeistert, auch jenseits elektronischer Netzwerke);
- T*echnikdistanzierte Bürger* (Kontrollgruppe, altersgemischt);[148]
- *Professionelle Experten*, zum Beispiel IT-Sicherheitsspezialisten, Datenschützer.

Sichtbar gemacht werden sollen die Privatheitsvorstellungen, etwaige Befürchtungen und Sicherheitszweifel eben dieser Gruppen. Als Methode setzen wir Fokusgruppen-Interviews ein. Diese werden im Folgenden erläutert.

1.5.2 METHODE

Um Antworten auf die Forschungsfrage zu erhalten, werden Fokusgruppen-Interviews durchgeführt. Es handelt sich bei letzteren um eine qualitative Forschungsmethode, die bevorzugt dann Anwendung findet, wenn die Realitäten und Erfahrungen verschiedener Akteure sichtbar gemacht werden sollen:

> *„Focus groups have proven helpful mostly because they provide an interactive environment. Focus groups enable people to ponder, reflect and listen to experiences and opinions of others. This interaction helps participants to compare their own personal realities to those of others."*[149]

Fokusgruppen-Interviews bieten sich folglich insbesondere für die Identifizierung sozialer Aushandlungsprozesse und Konflikte an, sie eignen sich perfekt zur Untersuchung von (unterschiedlichen) Vorstellungen zu einer Thematik:

„Focus groups interviews should be considered when:

- You are looking for a range of ideas or feelings people have about something.
- You are trying to understand differences in perspectives between groups or categories of people. [...]
- The purpose is to uncover factors that influence opinions, behavior or motivation. [...]
- You want ideas to emerge from the group. A group possesses the capacity to be more than the sum of its parts, to exhibit a synergy that individuals alone don't possess."[150]

In diesem Sinne lassen sich über Fokusgruppen-Interviews gesellschaftliche Konflikte und Normenbildungen identifizieren. Daneben werden in solchen Interviews nicht nur die Normen selbst sichtbar, sondern auch andere gesellschaftliche Werthaltungen, mit denen diese Normen in Widerspruch stehen. An den im Fokusgruppen-Interview zutage tretenden Konflikten lassen sich ganz im Sinne Soloves insofern Privatheitsnormen identifizieren, als in diesen Privatheits-*Probleme* thematisiert werden.

---

148 Unsere Gruppenbildung stimmt mit aktuellen repräsentativen Erkenntnissen überein. So wurden in einer nach Abschluss unserer eigenen Untersuchung vom Deutschen Institut für Vertrauen und Sicherheit im Internet (DIVSI) veröffentlichten (qualitativ und quantitativ verfahrenden) Milieu-Studie zu Vertrauen und Sicherheit im Internet die Gruppen „Digital Natives", „Digital Immigrants" (bei uns Affine) und „Digital Outsiders" (bei uns Distanzierte) gebildet (wobei innerhalb der Gruppen noch einmal in Sub-Gruppen unterteilt wurde). Vgl. DIVSI 2012, S. 16.

149 Krueger / Casey 2009, S. 12.

150 Krueger / Casey 2009, S. 19.

Um die soziale Realität von Akteuren (zum Beispiel von Internetnutzern) sichtbar zu machen, diskutieren mehrere Teilnehmer problemzentriert und ergebnisoffen über ihre Erfahrungen, Vorstellungen, Werthaltungen und Bedürfnisse, wobei sich die Gruppe im Falle nicht-kommerzieller Forschung aus 6–10 Personen zusammensetzt.[151] Die jeweiligen Gruppen sollten eine gewisse Homogenität aufweisen, „but with sufficient variation among participants to allow for contrasting opinions."[152] Die Homogenität der Zusammensetzung der jeweiligen Gruppen wird dadurch garantiert, dass die Teilnehmer anhand eines Kriterienkatalogs (*screener*) ausgewählt werden.

Als Diskussionsanregung wird ein vom Interviewer vorab festgelegter Fragenkatalog abgearbeitet, der lediglich zur Stimulation der Diskussion dient; die Diskussion verläuft ergebnisoffen, weil das Ziel darin besteht, neue Erkenntnisse zu generieren.[153] Dies wäre mit Fragebogenerhebungen, die mögliche Antworten vorab festlegen, nicht in gleicher Weise möglich.

Die übliche Dauer einer Interview-Session beträgt zwei Stunden. In dieser Zeit sind normalerweise maximal zwölf Fragen zu behandeln, inklusive der eher aus technischen Gründen gestellten Eröffnungs-, Einführungs- und Schließungsfragen.[154] Die Gliederung der Leitfäden orientierte sich in unserem Fall an unserer Forschungsfrage (siehe oben); die in abstrakten Begriffen formulierte Fragestellung wurde in einfache, klare kurze und offene Interviewfragen überführt. Ergaben sich in den Interview-Sessions neue Fragerichtungen, so wurden ad hoc Nachfragen formuliert und es wurde vom Leitfaden abgewichen. Damit kommen wir zur Durchführung der Forschung.

1.5.3 DURCHFÜHRUNG

Pro Fokusgruppe wurden vier Interviews in vier Städten durchgeführt.[155] Um regionale Diversität nachzuzeichnen, wurden folgende Städte ausgewählt: Berlin, Leipzig, Frankfurt und Essen. Die Rekrutierung erfolgte wie üblich zeitnah zu den Interviews; sie wurde im Fall der Nutzergruppen von professionellen Rekrutierungsagenturen übernommen, die Teilnehmer an den Expertenrunden wurden von uns selbst gezielt rekrutiert. Zur Rekrutierung der Teilnehmer wurden finanzielle Anreize (*incentive*) gesetzt. Da es sich bei den Digital Natives, den Technikaffinen und den Technikdistanzierten um (mehr oder weniger versierte) Nutzergruppen handelt, waren die an diese gerichteten Fragen identisch. Demgegenüber wurde davon ausgegangen, dass die *Professionellen* aufgrund ihrer beruflichen Beschäftigung mit der Thematik nicht nur über andere Kenntnisse verfügen, sondern die Thematik auch stärker aus einer über-individuellen Sichtweise perspektivieren (als Anbieter von Sicherheitsdienstleistungen, als Fürsprecher des Datenschutzes etc.). Aus diesem Grunde kam bei diesen ein anderer Fragenkatalog zum Einsatz. Die Fokusgrupppen setzten sich in der Regel aus sechs bis acht Teilnehmern zusammen; zwei Ausreißer gab es bei den Expertenrunden: An einer nahmen nur drei Teilnehmer teil, an einer anderen dafür zehn.

Der Diskussionsverlauf wurde als Audiosignal mit digitalen Aufzeichnungsgeräten mitgeschnitten, die Auswertung der transkribierten Gruppeninterviews erfolgte inhaltsanalytisch.[156] Im Anschluss an die Vorrede durch den Interviewer (Rahmung des Interviews), wurde ein Frageleitfaden abgearbeitet. Dieser bestand aus zwölf Fragen: Auf die Eröffnungsfrage, Einführungsfrage (explizite Setzung des

151 Krueger / Casey 2009, S. 67-68.
152 Krueger / Casey 2009, S. 66.
153 Krueger / Casey 2009, S. 35-61.
154 Krueger / Casey 2009, S. 39-41.
155 Eine Ausnahme bildet hier die Fokusgruppe der Experten: Zum Zeitpunkt der Niederschrift dieses Textes waren Interviews lediglich mit drei Fokusgruppen durchgeführt worden (Berlin, Essen, Leipzig).
156 Vgl. Mayring 2008.

Themas) und Übergangsfrage (Von der Themensetzung zu den Kernfragen) erfolgte der Übergang zu den Kernfragen (Erfahrung von Verletzung der Privatheit online und offline; Vertrauen gegenüber technischer Komplexität; Wert(schätz)ung des Privaten online; Einschätzung von Risiko und Gefahr online; individuelle Kompetenzen zur Erzeugung von Privatheit online; Faktoren zur Generierung von Vertrauen online). Den inhaltlichen Abschluss bildete eine Übung (schriftliches Ranking vorgegebener Situationen der Privatheitsverletzung), mit der Schlussfrage wurde die Sitzung beendet.

Damit kommen wir zu den Ergebnissen der Forschung.

1.6 FORSCHUNGSRESULTATE: DIE PRIVATHEITSVORSTELLUNGEN DER NUTZER

Im Folgenden stellen wir erste Ergebnisse der Fokusgruppen-Interviews vor. Wir beginnen mit einer beschreibenden Charakterisierung der Privatheitsvorstellungen und Befürchtungen/Wünsche der Digital Natives (1.6.1), der Technikaffinen (1.6.2) und der Technikdistanzierten (1.6.3), um daraufhin die Perspektive der Experten darzustellen (1.6.4). Schließlich werden die Gemeinsamkeiten und Unterschiede bezüglich der Gruppen zusammengefasst und erste Folgerungen abgeleitet (1.6.5).

1.6.1 DIGITAL NATIVES

Jugendliche Nutzer sind nicht nur mit dem Internet aufgewachsen, sondern nutzen dieses auch mit großer Selbstverständlichkeit. Zweckgebundene (beruflich, für die Ausbildung/das Studium etc.) und eher private (Freizeit-)Nutzung fließen weitestgehend ineinander. Die Nutzung des Internets durch die *Natives* zielt (unter anderem) in hohem Maße auf die Pflege und den Erhalt sozialer Netzwerke sowie auf Unterhaltung ab. Bezüglich der Frequentierung von *Social Network Sites* (SNS) lässt sich ein regelrechter *Peer Group Pressure* diagnostizieren, insofern 94 Prozent der Nutzer dieser Altersgruppe auf SNS interagieren.[157] Folgerichtig berichteten jüngere Nutzer auch von erheblichen Nachteilen, mit denen sie sich bei Nicht-Nutzung von SNS konfrontiert sähen.

Während die Websites der SNS zum Teil immer im Hintergrund geöffnet bleiben, betonen die Digital Natives sehr stark die *individuelle Nutzerverantwortung*: In vielerlei Hinsicht trügen die Nutzer selbst die Verantwortung dafür, welche ihrer persönlichen Informationen im Internet wem zugänglich würden. Gleichwohl sei in vielen Fällen aber auch ein individuell unverschuldeter Kontrollverlust zu erfahren.

Privatheitsvorstellungen und -brüche online und offline

Es lässt sich keineswegs eine Erosion von Privatheitsvorstellungen (und -praktiken) auf Seiten der Digital Natives feststellen. Nicht nur für die „klassisch" als privat verstandenen Bereiche des eigenen Körpers und der eigenen Wohnung gilt bei den *Natives* nach wie vor die Norm, dass diese der eigenen Kontrolle zu unterliegen hätten. Im Falle des Körpers wird diesbezüglich auf ein physisches, ausdrücklich aber auch auf ein verbales Zu-Nahe-Treten durch andere Personen verwiesen, bis hin zu sexualisierter Gewalt. Die Intimität des Körpers sei in allen Fällen zu wahren. Diese Norm wird insofern auf das Internet übertragen, als sexualisierte Verbalattacken in Chatrooms genauso als Angriff auf die Intimität des Körpers gesehen werden, wie Aufdringlichkeiten im Zuge von Face-to-Face-Interaktion. Die eigene Wohnung gilt den Digital Natives insofern als privat, als diese einen von unerwünschter Beobachtung freien Interaktionsraum bilden solle: Beobachtetwerden gilt hier folglich als massive Störung der Privatheit und resultiere in einer halb-bewussten Verhaltensanpassung, vor der der eigene Wohnraum geschützt sein solle. Auch diese Norm wird auf das Internet übertragen, auch in diesem Kontext wird das unerwünschte Beobachtetwerden als Privatheitseingriff erachtet (dazu weiter unten).

In informationeller Hinsicht bestimmen die Digital Natives Privatheit dahingehend, dass Fremde über kein Wissen ihre

[157] BITKOM 2011, S. 4.

Person betreffend verfügen sollten (das heißt Wissen, das über die Wahrnehmung ihrer Erscheinung in der Öffentlichkeit der Diskothek, der U-Bahn usw. hinausgeht). Auch das In-Umlauf-Bringen von Falschinformationen bezüglich ihrer Person sowie die Weitergabe von persönlichen Informationen an Dritte gilt als Privatheitsbruch. In Bezug auf das Internet finden sich diese Privatheitsnormen in ähnlicher Form wieder. Das freie Flottieren von (damit auch für Fremden zugänglichen) persönlichen Informationen (die eigene Person oder den Partner betreffend) wird genauso abgelehnt wie die ungefragte Einspeisung von (Falsch-) Informationen durch Dritte (zum Beispiel, wenn Gerüchte in Umlauf gebracht werden oder Abbildungen ungefragt hochgeladen werden). Zu guter Letzt gilt der eigene Rechner in ganz ähnlicher Weise als privater Bereich, wie die Wohnung: Zugang sei in letzterem Fall durch exklusiven Besitz des Schlüssels zu regulieren, in ersterem Fall durch exklusive Kenntnis der Passwörter.

Befürchtungen und Wünsche

Aus den Privatheitsvorstellungen ergeben sich einige Befürchtungen und Wünsche, die die Digital Natives mit der Internetnutzung verbinden. Generell wird das Internet als unüberschaubare Komplexität wahrgenommen, der gegenüber die Kontrolle eigener Informationen nur sehr bedingt möglich sei. Die Einspeisung von Informationen durch Dritte sei nicht zu kontrollieren; das potenzielle Publikum sei diffus und anonym, die Betreiber letztlich unerreichbar; einmal eingespeiste Informationen seien unmöglich wieder aus dem Netz zu entfernen, da die Verlinkung zur unkontrollierbaren Verbreitung führe. An diesem Punkt wurde vor allem eine Furcht vor der Vermischung von Handlungsfeldern sichtbar. Wenn beispielsweise Aktivitäten im Sportverein fotografiert, die Fotografien mit Namen versehen und vom Sportverein ins Netz gestellt werden, dann werden damit Informationen durch Dritte eingespeist. Die Informationen sind dann von einem quasi-unbeschränkten Publikum abrufbar. Durch das Zusammenspiel verschiedener Anwendungen (Website des Sportvereins und Suchmaschinen) ist die Information gleichzeitig von potenziellen Arbeitgebern auffindbar. Abgesehen davon, dass Nutzer damit die Möglichkeit verlieren, ihr Erscheinungsbild zu kontrollieren (das wurde in Bezug auf Fotos vielfach beklagt), wird so der als privat erachtete Bereich der Freizeitaktivitäten mit dem Bereich des „Arbeitslebens" vermischt: Die Trennung zwischen dem Publikum des Freizeit- und des Arbeitsbereichs bricht zusammen. Die Digital Natives befürchten, dass ihnen daraus Nachteile erwachsen. Arbeitgeber würden auf diese Weise nicht nur Kenntnis über ihre berufliche Person, sondern auch über ihre private erhalten, Falschinformationen könnten die Meinungsbildung manipulieren, die Wahrscheinlichkeit einer fairen Anstellungsentscheidung sinke. Dazu käme das Problem, in der Gegenwart immer für die gesamte (Internet-)Biographie geradestehen zu müssen. Da das Internet „nichts vergesse", würde man auch noch nach zehn Jahre alten Informationen beurteilt, ein Problem, wenn die Informationen im Internet etwa Jugendsünden beträfen.

Auch die Befürchtung, beobachtet und identifiziert zu werden, tritt bei der Internetnutzung auf – und zwar paradoxerweise unterschwellig und doch in verschärfter Form, sofern das Beobachtetwerden den Natives zufolge unter Umständen gar nicht bemerkt werden kann (*Hacking*, Viren, Trojaner). Auffällig ist, dass sich diese Befürchtung bei den Natives in erster Linie auf *andere Nutzer* bezieht, etwa andere SNS- oder Suchmaschinennutzer oder Hacker. Das Denken der Natives wird insofern bestimmt von der Figur eines Netzwerks, welches sich aus verstreuten Individuen zusammensetzt. Gefahren, die innerhalb des Netzwerks auftauchen können, sind dementsprechend Individuen zuzuschreiben; auch ist diesen Gefahren individuell entgegenzutreten. Folgerichtig finden die Natives es tendenziell kaum problematisch, wenn Betreiber ihre Daten *speichern*, sofern sie selbst deren *Verbreitung* kontrollieren können. Den Erhalt von Profilwerbung thematisieren die Natives vor allem bezüglich des Effektes als negativ („nervig"), die darunter liegenden Praktiken der Datensammlung und -korrelation

sowie der Profilbildung werden nur allgemein thematisiert – man weiß, dass die Betreiber mit den Daten arbeiten, man weiß aber weder, was diese genau machen noch was sie damit anfangen können und dürfen. Profilwerbung und dergleichen gilt folglich als notwendiges und kaum bemerkenswertes Übel, dem individuell zu begegnen sei – das eigene Kauf- oder Suchverhalten zum Beispiel sei ohnehin wenig interessant und daraus kaum etwas abzulesen.

Dementsprechend beziehen sich die Wünsche der Digital Natives vor allem auf die Kostenfreiheit und gute Bedienbarkeit der *Privacy Settings* und Sicherheitseinstellungen der Betreiber sowie auf besser nachvollziehbare AGBs. Das Wissensniveau hinsichtlich der technischen Schutzmöglichkeiten sowie der eigenen Rechte und der der Betreiber variiert mit dem Zeitaufwand, den die Natives in die Kompetenzbildung investieren (können): Da Zeit bei ihnen – so wie bei allen anderen Nutzergruppen auch – ein knappes Gut darstellt, berichten die Nutzer zum Teil über ausgefeilte, zum Teil über wenig fortgeschrittene Schutzpraktiken.

Zusammengefasst perspektivieren die Digital Natives auftretende Privatheitsprobleme im Internet tendenziell als individuelle Problematik und thematisieren die Internetnutzung zwar teilweise als Kontrollverlust, gehen mit diesem aber tendenziell recht gelassen um.[158]

1.6.2 TECHNIKAFFINE NUTZER

Auch bei den Technikaffinen fließen die private und berufliche Nutzung des Internets ineinander. Ihre Nutzung zielt auch, wenngleich weniger stark als bei den Digital Natives, auf die Pflege sozialer Netzwerke und auf Unterhaltung ab. Chatrooms und SNS werden weniger intensiv oder gar nicht genutzt, daneben finden sich mindestens gleichberechtigt die Rezeption von Nachrichten, der Zweck der Weiterbildung, eCommerce-Aktivitäten und dergleichen. Während das *Peer Group Pressure* zur Teilnahme an SNS in dieser Gruppe weitaus weniger ausgeprägt ist, schreiben auch die Technikaffinen dem individuellen Nutzer in hohem Maße die Verantwortung für die Kontrolle persönlicher Informationen zu und sehen sich im Internet mit einer nicht nachvollziehbaren technischen Komplexität konfrontiert. Bei den Technikaffinen ist das Bewusstsein für die massive Datensammlung im Internet sehr stark ausgeprägt, geht aber mit einem relativ starken Vertrauen in die eigene Kompetenz einher.

Privatheitsvorstellungen und -brüche online und offline

Auch bei den Technikaffinen lässt sich bei der Beschreibung der Privatheitsvorstellungen am Körper ansetzen. Dessen Unversehrtheit gelte es zu garantieren, jedoch mit Einschränkungen. Träten Beamte einer Person im Zuge der Durchsuchung zu Fahndungszwecken nahe, dann stelle dies zwar einen Eingriff in die Privatheit der Intimität des Körpers dar, jedoch einen legitimen. Auch der eigene Wohnraum gilt als privater Bereich, und zwar aus verschiedenen Gründen. Erstens bestehe hier das „right to be left alone", das heißt, das Betreten dieses Raumes habe genauso der persönlichen Kontrolle zu unterliegen, wie Möglichkeit der Beobachtung dieses Raumes durch andere Akteure. Zweitens stelle auch eine ungefragte Kontaktaufnahme in (oder an der Schwelle zur) Wohnung eine Verletzung der Privatsphäre dar, so zum Beispiel beim Erscheinen von Vertretern oder Verkäufern an der Wohnungstür. Diesbezüglich erstreckt sich der Privatheitsbruch nicht nur auf physische Anwesenheit von anderen Personen, sondern auch auf die Kontaktaufnahme per Telefon. Adresse wie Telefonnummer gelten bei eigener Nicht-Veröffentlichung als private Information. Erfolgt nun eine ungebetene Kontaktaufnahme, dann hängt die Bewertung des Vorgangs nicht zuletzt von der Intention des Kontaktaufnehmers ab. Der Versuch der Kontaktaufnahme durch unbekannte Personen gilt

158 Dies deckt sich mit zentralen Befunden der DIVSI-Milieu-Studie zu Vertrauen und Sicherheit im Internet. Dort heißt es: „Diejenigen Personen, die mit der Verbreitung des Internets aufgewachsen sind, neigen aufgrund ihres selbstverständlichen Umgangs mit dem Medium dazu, die Gefahren und Risiken zu unterschätzen. [...] Digital Natives zeigen nur wenig Verständnis für die Problematik von unerfahrenen Internetnutzern: In erster Linie steht der Nutzer selbst in der Pflicht, seine Aktivitäten im Netz zu verantworten (Selbstverschuldungsprinzip)." DIVSI 2012, S. 17.

beispielsweise dann als Privatheitsbruch, wenn diese eine Kaufentscheidung oder den Abschluss eines Vertrages herbeizuführen versuchen. Privatheit meint hier also auch, dass das individuelle Treffen von Entscheidungen nicht willentlich beeinflusst oder gar manipuliert werden soll. Sowohl die Kontaktaufnahme als auch der ungebetene Erhalt von Information gilt bei Zuwiderhandlung als Privatheitsbruch. Der Erhalt von Werbung wird also als Privatheitsbruch gesehen, im Falle von Postsendungen jedoch als äußerst schwacher und somit zu vernachlässigender Eingriff. Das Stichwort der Privatheit der Adresse weiter oben deutet schon an, dass die Technikaffinen auch die Weitergabe von persönlichen Informationen an Dritte als Privatheitsbruch definieren. Dies sei beispielsweise dann der Fall, wenn Informationen an Bekannte vermittelt würden und diese die Informationen dann an Dritte weitergäben.

Der von den Affinen aus normativen Gründen abgelehnte ungebetene Erhalt von Informationen (mit dem Ziel der Entscheidungsmanipulation) erhält aus ihrer Sicht im Internet eine neue Dynamik. Während Werbung per Post noch toleriert und teilweise als praktisch nutzbringend erfahren wird, gilt die Bombardierung mit Informationen zu Werbezwecken als massiver Eingriff – und dies umso mehr, wenn sie sich an die ebenfalls als privat geltende E-Mail-Adresse richtet. Aber ob persönlich adressiert oder nicht: Die Nutzer beklagen zum Teil einen seitens der Anbieter bewusst herbeigeführten kognitiven Overload, der das Ziel verfolge, ihre Kaufentscheidungen zu manipulieren. Die Norm der „freien Entscheidung" hat also online wie offline Gültigkeit, und das gleiche gilt für persönliche Informationen generell. Die Technikaffinen sehen die Einhaltung der Privatheitsnormen im Internet gleichzeitig als wichtiger und als schwieriger zu bewerkstelligen an, da das Internet bekannten, normativ geregelten Praktiken neue Dynamik verleihe: Das ungefragte Einstellen einer digitalen Abbildung ins Internet gilt zum Teil als schwerer Eingriff, während die ungefragte Weitergabe von Papierfotos gar nicht erst thematisiert wird. Zwar kommt es in beiden Fällen zum Verlust der Kontrolle über das eigene Erscheinungsbild, Verlinkung birgt aber die Möglichkeit einer viel weiteren Verbreitung. Zu guter Letzt gilt nicht nur das ungefragte Einspeisen von persönlichen Informationen durch Dritte als Privatheitsbruch – als Äquivalent zur Weitergabe persönlicher Informationen offline – sondern auch die Speicherung persönlicher Informationen, allerdings sind die Technikaffinen diesbezüglich überaus ambivalent.

Befürchtungen und Wünsche

Generell gleichen sich die Befürchtungen und Wünsche mit denen der Digital Natives in einer Vielzahl von Punkten. Die Unterschiede bestehen weniger hinsichtlich der Typen der vorgebrachten Befürchtungen, als bei der Perspektivierung dieser und beim Umgang mit diesen. Auch die Technikaffinen sehen sich einer anonymen technischen Komplexität gegenüber und die unkontrollierbare Verbreitung einmal eingegebener persönlicher Informationen als genauso problematisch an, wie deren Einspeisung ins Internet durch Dritte; auch sie nehmen die Betreiber als letztlich unerreichbar an und fürchten eine Vermischung von Handlungsfeldern. Die Technikaffinen haben aber aufgrund ihres höheren Alters in puncto Reputation und ökonomische Ressourcen tendenziell mehr zu verlieren. Im Netz auffindbare persönliche Informationen können sich beispielsweise nicht nur auf sie selbst, sondern auch auf ihr familiäres Gefüge negativ auswirken; da sie über größere ökonomische Ressourcen verfügen, können sie auch höhere Verluste beklagen. Folgerichtig agieren sie mit größerer Vorsicht und gehen tendenziell geringere Risiken ein. Während sich die Privatheitsvorstellungen also stark ähneln, erfahren diese bei den Technikaffinen eine *stärkere Gewichtung*.

Ein ganz entscheidender Unterschied besteht in Bezug auf die Zur-Kenntnisnahme der Rolle der Betreiber. Die Technikaffinen nehmen diese *als Akteure mit eigener Agenda* wahr, weshalb deren Praktiken in ihren Überlegungen eine größere Rolle spielen. In der Folge beziehen sie ihre Privatheitsvorstellungen nicht nur auf *andere Internetnutzer*, sondern

eben auch auf *die Betreiber*. Das gleiche gilt für die Befürchtung des Beobachtetwerdens. Die Technikaffinen rücken dementsprechend die Sammlung, Weiterverarbeitung und Weitergabe ihrer persönlichen Informationen in den Vordergrund. Zwar kennen auch sie nicht die genauen Betreiberpraktiken – das heißt, sie wissen nicht, welche ihrer Informationen von wem gespeichert, wie weiterverarbeitet und an wen weitergegeben werden – ein grundsätzliches Bewusstsein dafür ist aber vorhanden. Dies hat verschiedene Auswirkungen. Zum einen wird darauf mitunter mit einem Manipulationsverdacht reagiert: Seitens der Betreiber werde gezielt Begehren erzeugt, man werde „verleitet" und „verführt." Auch dem ungebetenen Erhalt von Informationen, das heißt hier von Profilwerbung oder Produkthinweisen, stehen die Technikaffinen wesentlich kritischer gegenüber, als die Digital Natives – und zwar weil in ihrer Vorstellung nicht nur der Eingang von Werbung (welche relativ leicht zu ignorieren sei) als Effekt eine Rolle spielt, sondern auch die Praxis, die diesen Effekt hervorruft: die Auswertung gespeicherter Suchanfragen, die Analyse von Kaufverhalten etc. Nicht alle Technikaffinen sehen diese Praxis und ihre Effekte indes kritisch; das Unterbreiten alternativer Angebote beim Online-Shopping weise zum Beispiel einen ansehnlichen praktischen Nutzen auf. Nutzer, die diesen praktischen Nutzen betonen, verkaufen indes nicht einfach ihre Privatheit für günstigere Angebote im Sinne des „privacy paradox";[159] es handelt sich vielmehr um Nutzer, die die Privatheitsproblematik als eine rein individuelle begreifen. Dementsprechend betrachten sie Datensammlung deshalb als unproblematisch, weil sie die individuellen persönlichen Informationen, die sie liefern als unsensibel einstufen – sie fokussieren also lediglich auf den *Informationstyp* und begreifen sich selbst als *Kunden*. Demgegenüber stehen Nutzer, die sich als *Bürger* verstehen und die Praktiken der Betreiber als Teil eines gesellschaftlichen Handlungszusammenhangs einordnen. Ihre Befürchtung besteht in der Entstehung eines „gläsernen Menschen": Beispielsweise könnten Profile des Kaufverhaltens in ein anderes Handlungsfeld wandern, etwa an Krankenkassen gehen, welche dann Risikopatienten ausfiltern. Daraus ergeben sich zwei Wünsche: Der erst betrifft die Transparenz der Betreiberpraktiken: Die Betreiber müssten kenntlich machen, was mit den persönlichen Informationen der Nutzer geschehe – und zwar nicht nur in Form von AGBs, die zu lang, kompliziert, unverständlich seien und die Nutzer mit einem „take it or leave it"-Ansatz konfrontierten. Zweitens besteht vielfach der Wunsch, den Betreibern die Möglichkeit der Speicherung, Verarbeitung und Weitergabe von Informationen und das Anlegen von Profilen untersagen zu können, ohne dass die Nutzung der Anwendungen deshalb abgelehnt wird. Sofern dies bereits möglich ist – und auch die Technikaffinen kennen diesbezüglich weder die Rechtslage noch die technischen Möglichkeiten – besteht der Wunsch, dass die Betreiber diese Möglichkeit deutlicher, ihre Anwendungen mit besserer *Usability* ausstatten und dass das Problem „unverdaulicher" AGBs gelöst wird.

Zusammengefasst begreifen die Technikaffinen Privatheit im Internet verstärkt als gesellschaftliches Problem, haben aber trotz aller Befürchtungen eines Kontrollverlustes so viel Vertrauen in ihre Kompetenzen, dass sie das Risiko des Agierens im Internet bei vorsichtiger Nutzung als tragbar einstufen.[160]

1.6.3 TECHNIKDISTANZIERTE NUTZER

Technikdistanzierte Nutzer weisen ein überaus vorsichtiges Nutzungsverhalten auf. Die Nutzung dient bei ihnen nur selten dem Zweck, soziale Netzwerke aufrechtzuerhalten.

[159] Zum „privacy paradox" vgl. Acquisti / Grossklags 2003. Anzumerken bleibt, dass genau die Nutzer, die den praktischen Nutzen betonen und Privatheit hintanstellen gleichzeitig Anbietern die Treue halten, bei denen sie (wissentlich!) *mehr bezahlen* ***und*** obendrein auch noch (wissentlich!) *mehr* persönliche Informationen herausgeben. Ihr Verhalten gestaltet sich also wesentlich komplexer als eine individuelle Kosten/Nutzen-Kalkulation, sofern die soziale (kollektive!) Konstruktion der Marke hierbei eine Rolle spielt.

[160] Um unsere Analyse auch hier quantitativ zu unterfüttern: Bei den Technikaffinen „besteht ein grundsätzliches Problembewusstsein und eine damit verbundene erhöhte Risiko-Wahrnehmung". Vgl. DIVSI 2012, S. 17.

Hinsichtlich sozialer Interaktion empfinden sie das Internet geradezu als defizitär, insofern Interaktion (unmittelbares Feedback) nur sehr bedingt möglich sei; das Internet als solches sei anonym und unpersönlich, Internet-gestützte soziale Netzwerke und virtuelle Freundschaften seien letztlich nicht real. Während auch bei den Technikdistanzierten die private und berufliche Nutzung tendenziell ineinander übergeht, gestaltet sich bei ihnen auch die private Nutzung in erster Linie als zweckgebunden: Sie rufen Informationen ab (Nachrichten, Recherchieren), buchen Reisen oder suchen Fahrpläne und Veranstaltungskalender auf. Chatrooms, Foren, und SNS spielen für sie kaum eine Rolle, Kommunikation betreiben sie im Internet äußerst vorsichtig, denn im Internet bleibe „alles hängen". Für kommerzielle Transaktionen (Online-Banking, eCommerce) sind sie dahingegen mitunter offen, da den Betreibern Vertrauen entgegengebracht wird (Banken, bekannte Online-Händler). Daran zeigt sich, dass die Technikdistanzierten grundsätzlich sehr stark den „klassischen" Mechanismen der Vertrauensbildung verhaftet sind, sie vertrauen Institutionen und Marken. Der Virtualisierung aller möglichen Lebensbereiche wird dagegen wenig Vertrauen entgegengebracht, diese und insbesondere das Internet überfordere den Einzelnen strukturell.

Privatheitsvorstellungen und -brüche online und offline

Die Technikdistanzierten sehen in ungewollter Kontaktaufnahme einen massiven Eingriff in die Privatsphäre. Verkaufsgespräche oder der Versuch, um ihre Mitgliedschaft zu werben, werden als nicht zu tolerierende Aufdringlichkeit gewertet. Dies gilt sowohl an der Wohnungstür: Kontaktaufnahme als Verletzung des physischen Privatbereichs der Wohnung. Doch auch bei der ungewollten Kontaktaufnahme am Telefon, auf der Straße, in der U-Bahn oder im Supermarkt fühlen die Technikdistanzierten sich in ihrer Privatheit verletzt. Während sie mit diesem Verständnis Parallelen zu den Technikaffinen aufweisen, betonen sie den Grad solcher Privatheitsverletzungen ungleich stärker. Sie legen damit ein sehr ausgeprägtes Bedürfnis Privatheit als solcher und nach „privacy in public" an den Tag. Die Weitergabe oder der Verkauf von Adress- und Telefondaten wird als Ausverkauf von Privatheit gewertet. Sie thematisieren damit sowohl die ungewollte Verknüpfung von Operationsketten wie auch die ungewollte Herausgabe und den ungewollten Erhalt von Informationen als Privatheitsbruch. Während ihre Privatheitsvorstellung (genau wie bei den anderen Gruppen) keinesfalls eine räumliche ist, lehnen sie auch die Lokalisierung ihres Aufenthaltsortes und die einseitige Beobachtung ihres Verhaltens als Eingriff ab. Die Privatheitsvorstellungen der Technikdistanzierten beziehen sich also nicht auf gänzlich andere Gegenstände oder Situationen als die der anderen Gruppen; jedoch wird Privatheit, verstanden als Gut, noch stärker gewichtet als bei den anderen Nutzern.

Bei der Übertragung der Privatheitsnormen auf das Internet sehen die Technikdistanzierten diese im Kontext zahlreicher Anwendungen verletzt. Genannt werden beispielsweise die mögliche Lokalisierung des Aufenthaltsortes über *Smartphones*, die Beobachtung des Verhaltens über Statusmeldungen auf SNS (wird daher beides nicht genutzt) und die Weitergabe der E-Mail-Adresse. Letzteres wird als noch massiverer Eingriff angesehen, als die Weitergabe der Postadresse, da sie per E-Mail mit Spam und ungebetener Werbung bombardiert werden könnten. Letzteres wird wiederum als ungebetene Kontaktaufnahme und ungebetener Erhalt von Informationen betrachtet und daher rundheraus abgelehnt. Profilwerbung unterziehen die Technikdistanzierten durch die Bank mit massiver Grundsatzkritik – das gilt erst recht für die zugrunde liegenden Praktiken des Speicherns, Verarbeitens und der Weitergabe von als persönlich erachteten Informationen.

Befürchtungen und Wünsche

Persönliche Informationen werden von den Technikdistanzierten im Internet als grundsätzlich gefährdet angesehen, weil diese genauso grundsätzlich nicht löschbar seien. Die Weiterleitung von Daten sei vollkommen unkontrollierbar, ebenso der Verkauf dieser. Das Publikum sei anonym, der Rezipient der Informationen nur schwer bestimmbar. Dies

könne dann zur Verletzung der persönlichen Integrität im Offline-Leben führen, wenn „gefährliche Personen" die persönlichen Informationen erhielten und Kapital daraus schlagen würden (der berühmte Einbruch in die Wohnung bei öffentlicher Mitteilung, verreist zu sein). Auch die Technikdistanzierten sehen wiederum einen Kontrollverlust dadurch gegeben, dass Dritte Informationen ins Internet einspeisen können, und hegen die Befürchtung, dadurch identifizierbar zu sein, dass verschiedene Anwendungen verknüpft werden. Die stärkste Sorge verbinden die Technikdistanzierten jedoch nicht mit den Praktiken anderer Nutzer, sondern mit denen der Betreiber. Der unbegrenzten Speicherung, Weitergabe und Verarbeitung persönlicher Informationen gelten die größten Befürchtungen, denn eben dadurch würden die Nutzer einseitig beobachtbar. Die genannten Praktiken würden beispielsweise die Zusendung von Profilwerbung per E-Mail ermöglichen, und Absender würden erfahren, ob, wann und wie lange solche E-Mails geöffnet und betrachtet würden. Daraus ergeben sich die schon bekannten Wünsche, die von den Technikdistanzierten aber mit noch größerem Nachdruck geäußert werden: der Wunsch nach einer Transparenz der Betreiberpraktiken, der Wunsch, die Betreiber erreichen und diesen die Speicherung, Verarbeitung und Weitergabe von Informationen untersagen zu können, der Wunsch nach Transparenz und Kenntnis der technischen Kontrollmöglichkeiten, höherer Kompetenz sowie nach einer besseren Kenntnis der Rechtslage, der Wunsch nach Reversibilität (endgültiges Löschen), der Wunsch, ungebeten keine Information zu erhalten und der Wunsch, mehr Kontrolle über Abläufe zu erhalten.

Zusammengefasst begreifen die Technikdistanzierten Privatheit im Internet als gesellschaftliches Problem und verfügen zudem über eher geringe Kompetenzen. Von allen drei Gruppen weisen sie eindeutig das größte Unbehagen bezüglich eines gefühlten Kontrollverlustes auf und gestalten ihr Nutzungsverhalten aus diesem Grunde wenig risikofreudig.[161]

1.6.4 EXPERTEN

Von allen befragten Gruppen nehmen die (IT-Sicherheits- und Datenschutz-)Experten die weiteste Perspektive auf das Internet und damit in Beziehung stehende Privatheitsprobleme ein. Das Internet wird in die zeitliche Trajektorie einer medientechnologisch getriebenen Zivilisationsgeschichte eingebettet, wobei der Mensch als anthropologisch konstante Entität porträtiert wird, insofern dieser immer die gleichen Bedürfnisse aufweise (etwa nach Nähe, Kommunikation und Gemeinschaft). Der Mensch habe es gelernt, mit den sich wandelnden Umständen umzugehen, die konstanten Bedürfnisse also mit jeweils andersartigen Mitteln zu befriedigen. Das Aufkommen neuartiger Problemlagen sei dem „technischen Fortschritt" ein gutes Stück weit inhärent und insofern nichts Neues. Wiederholt führen die Experten eine Denkfigur an, die sich als das „arms race"-Argument bezeichnen lässt: Die Technik entwickele sich ständig weiter, mitunter, bis es zu erheblichen sozialen Verwerfungen komme; die Reaktion darauf, etwa in Form der Erfindung angemessener Datenschutzregelungen, Nutzer-Kompetenzniveaus und Umgangsnormen, erfolge zum Teil erst im Rahmen eines nachholenden Lernprozesses. Die Geschwindigkeit des Wandels sei allerdings mittlerweile so enorm hoch, dass die nachholende Regulierung Gefahr laufe, immer schon zu spät zu kommen. Während sich die Experten bei der Spekulation bezüglich der Ausbildung konsistenter Praktiken in der Zukunft in der Tendenz als optimistisch erweisen, sind sie bei der Bewertung der aktuellen Situation indes eher kritisch-pessimistisch. So finden sich zweierlei Formen der Bewertung der aktuellen und zukünftigen Situation:

- Zutrauen in die Lernfähigkeiten des Menschen und in dessen Vermögen, machtvollen soziotechnischen Strategien schlaue Alltagstaktiken entgegenzusetzen
- Pessimistische Bewertung von Internet-bezogenen Sozialitätsformen als sozialer Rückschritt

[161] Bei den „Digital Outsiders" (von uns „Distanzierte" genannt) „überwiegt eine distanzierte Einstellung, bedingt durch geringe Interneterfahrung und somit eine generelle Unvertrautheit mit dem Medium. Zahlreiche Internetdienstleistungen werden daher von diesen Gruppen nicht in Anspruch genommen." Vgl. DIVSI 2012, S. 17.

Die gesellschaftliche Perspektivierung der Experten zeigt sich auch daran, dass die Praktiken der Speicherung, Weiterverarbeitung und Weitergabe von Daten durch die Betreiber – kritisch „Datensammelwut" genannt – historisch auf das Aufkommen statistisch-basierten Marketings zurückgeführt werden. Mit dem Internet weite sich diese Praxis so sehr aus, dass sie eine neue Qualität erhalte. Zwar geben die Experten an, dass auch sie nicht die konkreten Praktiken der Betreiber von Internetanwendungen (aufgrund der mangelnden Transparenz derselben) kennen würden, doch haben sie detaillierte Kenntnisse bezüglich der technisch möglichen Prozessierweisen, der rechtlichen Lage und der Geschäftsmodelle der großen datenzentrierten Dienste. Indem sie all dies als Teil eines zivilisationsgeschichtlichen Prozesses betrachten, perspektivieren sie Internet-bezogene Praktiken grundsätzlich als soziokulturelles Phänomen. Im Folgenden beschreiben wir die Probleme, die die Experten in Bezug auf solche Praktiken identifizieren.

Problematisierungen

Auch die Experten beziehen ihre Problematisierungen auf den informationellen Dreiklang der Speicherung, Verarbeitung und Weitergabe von Informationen. Dabei thematisieren sie die Rolle der Betreiber und anderer Nutzer auf differenzierte Art und Weise. Sie lassen überdies keinerlei Zweifel daran, dass das Interesse der Betreiber einzig und allein dem Zugang zu persönlichen Informationen gelte. Trotz genauer Kenntnis des technisch Möglichen seien sowohl die Praktiken der Betreiber als auch eine Großteil der soziotechnischen Prozesse im Internet letztlich vollkommen intransparent. Die Nutzer hätten aus den verschiedensten Gründen lediglich bei der Eingabe von persönlichen Informationen eine relative Kontrolle:

- Die Verknüpfung von Operationsketten, das heißt welche Informationen an welche Instanz fließen, sei grundsätzlich nicht zu kontrollieren (dies verschärfe sich mit Cloud Computing zusätzlich); zudem seien Informationen in Form von Daten beliebig oft weiterzuverarbeiten;
- die Eingabe von Informationen durch Dritte sei ebenso unkontrollierbar, außerdem würden auch Informationen von Akteuren, die sich gar nicht im Internet bewegen, gesammelt, verarbeitet und ausgewertet (zum Beispiel beim Tagging von Bildern);
- die Löschung einmal preisgegebener Informationen sei nicht möglich;
- durch die Akkumulation von in verschiedenen Kontexten eingegebenen Informationen könnten Datensammler akkurate Nutzerprofile erstellen, unsensible Daten würden durch Relationierung sensibel; dies könne zu Diskriminierung führen;[162]
- die Agency (Handlungsmacht) der Technologien, das heißt deren Fähigkeit, unterhalb der Wahrnehmungsschwelle der Nutzer eigenständig Prozesse zu initiieren und auszuführen.

Die so weit vorgebrachten Probleme wurden, wie weiter oben ausgeführt, auch von den Nutzern thematisiert und sind insofern bekannt. Gleichzeitig identifizieren die Experten aufgrund ihrer Erfahrung jedoch auch Probleme, die die Nutzer ihrerseits nicht erkennen (können). Wie ebenfalls oben angemerkt, tendieren beispielsweise die Digital Natives dazu, die Rolle der Betreiber im Zuge des Privacy-Management auszublenden oder durch diese erzeugte Privatheitsgefährdungen mit Verweis auf die Harmlosigkeit der eingespeisten Informationen abzutun. Die Experten machen dagegen deutlich, dass die – auch von den Natives selbst abgelehnte – Identifizierung von Personen durch avanciertes Data Mining und dergleichen auch dann möglich ist, wenn nur triviale Informationen eingegeben werden. Selbst die grundsätzlich wünschenswerte Pseudonymisierung und Anonymisierung böte hiervor nur noch bedingt Schutz. Darüber hinaus verweisen die Experten darauf, dass die Agenda der Betreiber in erster Linie durch deren Geschäftsmodell bestimmt wird. Während sich aufseiten

[162] Vgl. zur auf Profilbildung basierenden Diskriminierung Gandy 1993.

der Natives eine Ahnung findet, dass Betreiber mitunter Informationen weiterverarbeiten und -geben, weisen die Experten eben diese Tätigkeit als einziges oder zumindest als Hauptinteresse der Betreiber aus.

Zu betonen ist, dass die Problematisierungen, die die Experten in Bezug auf die Nutzer vornehmen, kaum oder nur selten als *Schelte* daherkommen. Vielmehr wird kritisiert, dass die Nutzer aus verschiedenen Gründen zu wenig Macht hätten. Das Hauptproblem bestehe darin, dass sie keine Vorstellung davon hätten, im Rahmen einer Informationsökonomie zu agieren: Da ihnen das Geschäftsmodell der Betreiber nicht bekannt sei, hätten sie kein Bewusstsein für den *Tauschhandel*, an dem sie teilnähmen. Dieser bestehe im Austausch kostenloser Dienste gegen Daten. Den Nutzern sei also nicht klar, dass jede *Hol-Bewegung* (zum Beispiel die Nutzung von Suchmaschinen) gleichzeitig eine *Bring-Bewegung* (Suche ermöglicht Rückschlüsse auf Person) darstelle; im Resultat fehle ihnen eine Vorstellung vom *Wert der eigenen Informationen*.

Die Experten sehen ein in mehrfacher Hinsicht asymmetrisches Verhältnis zwischen Nutzern und Betreibern:

- Die Betreiber kennen die Logik des Tauschhandels der Informationsökonomie, die Nutzer nicht;
- die Betreiber können die Praktiken der Nutzer beobachten, umgekehrt gilt das nicht;
- die Betreiber kennen die Rechtslage, die Nutzer keineswegs.

Dem von den Experten gezeichneten Bild zufolge agieren die Nutzer in diesem Sinne in einer gleichsam heimlichen Informationsökonomie, deren Bedingungen sie weder in ökonomischer noch in technischer und rechtlicher Hinsicht kennen. Daraus ergäbe sich eine Reihe von Problemen, welche sich aufseiten der Betreiber, der Nutzer, der Rechtsprechung und der Gesellschaft insgesamt verorten lassen.

Grundsätzlich bestünde eine Diskrepanz zwischen den Erwartungen der Nutzer und den von den Betreibern erzeugten technischen Skripten vieler Internetanwendungen (zum Beispiel das von den Nutzern nicht wahrgenommene Setzen von Flash-Cookies). Die Betreiber akzeptierten zudem bereits existierende Lösungen nicht als industriellen Standard (zum Beispiel *Do Not Track Header* zur Verhinderung von Tracking). Die Marktmacht der Betreiber ermögliche es diesen, politische Entscheidungen bezüglich des Datenschutzes zu beeinflussen (Lobbyismus), Anbieter technischer Lösungen zum Privatheitsschutz oder Halter großer Datenbestände einfach aufzukaufen. Die Globalisierung der Märkte führe schließlich dazu, dass das Tempo von Unternehmensverkäufen höher sei als die Möglichkeit technischer Re-Organisation: Man könne „die Daten gar nicht so schnell von den Rechnern bekommen, wie die Bude verkauft" sei.

Aufseiten der Nutzer bestünden die Probleme indes vor allem darin, dass diese beim Versuch, das Funktionieren der Informationsökonomie zu verstehen, überfordert seien. Mitunter sei eine mangelnde „Politisierung" (verstanden in einem weiten Sinne) zu konstatieren. Durch das asymmetrische Verhältnis entfalle die Möglichkeit, dass die Nutzer „mit den Füßen abstimmen" und zu einem anderen Anbieter wechseln, wenn der bisherige nicht die Privatheitserwartungen erfülle. Die Nutzer hätten schlicht keine Kenntnis darüber, ob ihre Privatheitsnormen den verwendeten Technologien eingeschrieben würden. Zum Beispiel würde niemand die AGBs lesen oder gar verstehen; die Nutzer bestimmter E-Mail-Dienste würden folglich einer kompletten inhaltlichen Auswertung ihres Postein- und -ausgangs zustimmen, ohne dass ihnen das bewusst sei. Würden sie dann dienstliche Informationen über einen solchen Account austauschen, dann wären diese Informationen damit an den Betreiber abgetreten, wozu sie gar nicht befugt seien. Zwar erführen die Nutzer nur selten einen individuell und situativ kausal zuzuordnenden Schaden; es sei jedoch bekannt, dass die Militärs bestimmter

Länder geschulte Mitarbeiter gezielt in den Betreiberunternehmen platzierten, um verdeckte Industriespionage zu betreiben. Neben solchen handfesten wirtschaftlichen Schädigungen würden die Nutzer im Übrigen aufgrund von Unkenntnis der rechtlichen Lage eher Selbst-Zensur betreiben, als ihr Auskunftsrecht wahrzunehmen. Die Entwicklung eines Problembewusstseins sei Voraussetzung für die dringend erforderliche Ausbildung von Medienkompetenz; letztere sei ihrerseits Voraussetzung für die Möglichkeit, fundierte Risikobewertungen vorzunehmen. Beispielsweise müsste den Nutzern stärker vor Augen geführt werden, dass sie mit einer fragmentierten Rechtslage konfrontiert seien: Zum einen gelte bei der Nutzung vieler Dienste die Rechtsprechung anderer Länder, zum anderen sei die Rechtsprechung bezüglich des Internets auch in nationalem Rahmen unterentwickelt. Die Nutzer seien die Delegation von Verantwortung an Instanzen gewohnt, die den Rechtsrahmen setzen und dessen Gültigkeit durchsetzen, und eben das entfalle im Internet.

Womit wir zur Rechtsprechung kommen. Diesbezüglich stellen die Experten zunächst fest, dass mittlerweile ein gesellschaftlicher Zwang zur Nutzung des Internets bestehe. Daraus erwachse dem Gesetzgeber die Aufgabe, die Festlegung der Nutzungsbedingungen nicht allein den Betreibern zu überlassen, sondern für einen angemessenen rechtlichen Rahmen zu sorgen. „Rechtlicher Rahmen" meint dabei keineswegs schlicht Verbote, vielmehr verliefen die Diskussionen entlang der Unterscheidung von Verboten und Anreizen. Während Auswüchse mit Verboten zu bekämpfen seien, sei die Wirksamkeit letzterer doch fraglich. Ein Verbot der Bewerberrecherche auf *Social Network Sites* durch Human Resource-Mitarbeiter sei etwa denkbar, in der Praxis jedoch kaum durchzusetzen. Grundsätzlich sei eher mit Anreizen zu arbeiten, beispielsweise mit Siegeln und dergleichen. In jedem Falle sei der rechtliche Rahmen im Internet unterentwickelt. Um hier Abhilfe zu schaffen, sei es beispielsweise denkbar, ein spezifisch auf das Internet bezogenes rechtliches Prinzip wie das der Sittenwidrigkeit zu entwickeln. Die Weitergabe von Informationen sei im Übrigen gar nicht oder nur bedingt geregelt, ein *praktikabler* rechtlicher Grundschutz für gewöhnliche Bürger müsse etabliert werden. Das größte und immer wieder betonte Problem hierbei stellt den Experten zufolge die Transnationalisierung, das heißt Überstaatlichkeit des Informationsflusses bei gleichzeitig national beschränkter Reichweite der Rechtsprechung dar. Eine einheitliche Datenschutzregelung sei mit dem Problem konfrontiert, dass hinsichtlich der bislang prozessierten Kultur-Programme (bestehende Privatheitsvorstellungen und -Normen) große Unterschiede sowohl innerhalb der europäischen Staaten als auch zwischen diesen bestehen.[163] Eine europaweite Datenschutzregelung müsse also an sehr unterschiedliche kulturelle Selbstverständlichkeiten anknüpfen. Der Informationsfluss sei indes staatlich nicht einzuhegen, daran hätten zum Beispiel Studien des Bundesministeriums für Bildung und Forschung keinerlei Zweifel gelassen.[164] Plädiert wurde daher für eine im besten Falle globale, mindestens aber europäische Datenschutzlösung.

Wir nähern uns damit der gesellschaftlichen Dimension des Problems an. Unter den Experten herrschte weitestgehend Einigkeit, dass das Problem der Privatheit im Internet letztlich kein technisches, sondern ein *soziales* darstelle. Aufgrund der Tatsache, dass diese Sicht von den Experten immer wieder als fundamental betont wurde, präsentieren wir ein längeres Zitat, dass diese Sicht zusammenfassend auf den Punkt bringt:

> *„Ich glaube, der erste Schritt wäre [...] anzuerkennen, dass es eben kein technisch lösbares Problem ist. Beispiel, wenn die Kinder größer werden, sagt man denen, nimm nichts von fremden Menschen, nichts*

163 Beispielsweise werden in Schweden persönliche Einkommen und Steuerzahlungen im Internet veröffentlicht.

164 Vgl. zum Beispiel Köhntopp / Köhntopp / Seeger 1997. Dass die Politik dennoch von Zeit zu Zeit die Illusion der technischen Regulierbarkeit propagiere (zum Beispiel Stoppschild), sei dem Versuch zuzuschreiben, Wählerstimmen einzufangen.

zu essen, nichts zu naschen, geh nirgendwo mit, lass dich nicht wegholen, das sagen die Leute denen, weil sie wissen, das Risiko ist da. Aber die sagen denen nicht, pass auf bei [SNS], oder geh nicht einfach ins Internet. […] Also die Menschen denken immer noch, das ist technisch lösbar, und solange keiner sich hinstellt und sagt, es ist nicht technisch lösbar, es ist ein gesellschaftliches Problem, so lange das nicht akzeptiert ist, passiert da auch wenig oder sehr langsam. […] wenn wir Experten oder alle Experten sagen, es ist so, und wissenschaftliche Arbeiten drüber schreiben, dauert es wie gesagt, 20, 30, 40 Jahre, bis diese Tatsache wirklich in der Bevölkerung ankommt. Und erst danach tut sich was, dann sagt nämlich die Mama zum kleinen Kind, pass auf bei [SNS], geh nur mit Pseudonym rein, und all so ein Kram, weil es dann einfach in der Gesellschaft durchgedrungen ist. Aber jetzt müssen die Leute sich schon hinsetzen und dafür vorbereitende Theorien schaffen. Und als Letztes noch: Wir haben Möglichkeiten, wie wir miteinander umgehen müssen, weil es das Problem ja seit Tausenden von Jahren gibt, dass man seinen Nachbarn nicht einfach erschlägt. Es gibt Religion, es gibt Grundlagen, über die wir verfügen, mit denen Menschen miteinander auskommen müssen. Bloß, man muss diese halt auch anwenden und wissen, dass man die anwenden muss, weil es eben keine andere Lösung und keinen anderen Schutz gibt."

Wie in dem Zitat angeführt, stellt *Internet Privacy* aus Expertensicht ein in sich heterogenes soziotechnisches Problem dar. Damit ist gemeint, dass das Gesamtproblem eine Reihe klassisch analytisch getrennter Aspekte aufweist. Es tritt sowohl auf Ebene der Technik (Normverletzende Prozessierungsweisen) als auch auf Ebene der Rechtsprechung (mangelnde rechtliche Regelung), der Akteure (mangelndes Wissen und Bewusstsein), der sozialen Organisation (keine ethisch fundierten Grundregeln der Informationsökonomie) usw. auf. Das Argument der soziotechnischen Problemlage betrifft den Experten zufolge also nicht nur die Regulierung von Betreiberpraktiken, sondern den soziotechnischen Alltag der Akteure in seiner Gänze. Zunächst sei die neue Situation erst einmal hinzunehmen (so wie es hinzunehmen sei, dass es hin und wieder regnet). Mit dem Internet entstehe eine neue Form von Gesellschaft, und das Bild, dass die Experten von dieser zeichnen, kommt dem Recht nahe, was Jean-Gabriel Ganascia als „Sousveillance Society" bezeichnet: Eine Gesellschaftsform, die charakterisiert ist durch „fundamental equality, which gives everybody the ability to watch – and consequently to control – everybody."[165] Symptom dafür ist das von den Experten angeführte Beispiel, dass beliebige Nutzer per gezielter Internetrecherche ein bis dato ungekanntes Maß an Informationen über andere Nutzer erlangen können. Rechtlich unbedenkliche, sozial jedoch fragwürdige Eigenschaften, wie etwa die Zugehörigkeit zu bestimmten Parteien, das Frönen bestimmter Freizeitaktivitäten oder das Aufweisen bestimmter sexueller Neigungen können dadurch leicht zu sozialer Stigmatisierung führen. Zwar betonen die Experten, dass dies gleichermaßen auch zur Ausbildung eines höheren Maßes an Toleranz führen könne, doch ist hier nicht entscheidend, welche Richtung die zukünftige gesellschaftliche Entwicklung tatsächlich nehmen wird. Wichtiger ist, dass dadurch die Wahrscheinlichkeit der Veränderung sozialer Strukturen heraufgesetzt wird. Die Experten plädieren vor diesem Hintergrund dafür, Wandel als solchen zu akzeptieren und am gesellschaftlichen Umgang mit dieser Situation zu arbeiten. Nur so könnten sich zivilisatorische Spielregeln entwickeln, und nur dies könne der Hoffnung Nahrung geben, dass aus dem Gemeinwesen heraus selbst-organisierte Alternativen zu den großen datenzentrierten Diensten entstünden, wie etwa dezentrale *Social Network Sites* und dergleichen.

Um zusammenzufassen: Die Experten wünschen sich einen für die Problematik hochgradig sensibilisierten Nutzertyp, ganz ähnlich den bei den Technikdistanzierten auffindbaren

[165] Ganascia 2010, S. 9.

Einstellungen, jedoch mit einem ungleich höheren Kompetenzniveau. Solche Nutzer könnten in einer Form von Gesellschaft, die das Internet als vollwertiges soziotechnisches Element integriert, so kontrolliert agieren, wie es in diesem Sozialitätstypus eben noch möglich sei. Die individuell nicht auffangbaren Kontrollverluste seien schließlich kollektiven Lösungen zuzuführen.

1.6.5 GEMEINSAMKEITEN, UNTERSCHIEDE, FOLGERUNGEN

Im Rahmen der Analyse ist deutlich geworden, dass sowohl die Privatheitsvorstellungen als auch die Befürchtungen und Wünsche der verschiedenen Nutzergruppen sich gleichzeitig stark ähneln und doch voneinander abweichen. Die zahlreichen Wiederholungen, die in der Analyse der verschiedenen Nutzerperspektiven auftauchen, verdeutlichen, dass alle Nutzer in abstrakten Termini das gleiche Bedürfnis haben: *Den Wunsch, ihre soziotechnischen Interaktionen und die dabei übermittelten Informationen kontrollieren zu können – nach Privatheit also*. Kontrolle meint dabei nicht das vollständige Bestimmen über jede Informationsprozessierung, sondern die Übereinstimmung letzterer mit den Normen und Erwartungen der Nutzer. Den Digital Natives ist es beispielsweise gleich, ob die Betreiber ihre Informationen *speichern*, sofern sie sie nicht *weitergeben*.

Wir kommen damit zu den Abweichungen zwischen den Gruppen. Hier ist vor allem zu berücksichtigen, dass das Kontrollbedürfnis der verschiedenen Gruppen unterschiedlich (stark) ausgeprägt ist. Die Digital Natives sehen den gefühlten Kontrollverlust bezüglich persönlicher Informationen vergleichsweise gelassen. Sie sind mit dem Internet aufgewachsen, verfügen über relativ hohe Kompetenzen (Kontrollmöglichkeiten) und agieren daher risikofreudig. Die beiden älteren Nutzergruppen der Technikaffinen und Technikdistanzierten artikulieren demgegenüber einen größeren Wunsch nach Kontrolle. Erstere weisen aber ebenfalls ein relativ hohes Kompetenzniveau auf, woraus sich eine Risiken sorgsam abwägende Nutzungsweise ergibt. Aus der Kombination eines ausgeprägten Privatheitsbedürfnisses und relativ niedriger Medienkompetenz erwachsen aufseiten der Technikdistanzierten die größten Befürchtungen. Die Digital Natives verleihen den Privatheitsnormen in Bezug auf andere Normen und Wünschen mit anderen Worten das geringste Gewicht. Das Verhältnis lässt sich wie folgt darstellen:

Tabelle 1: Verhältnis von Privatheitsbedürfnis und Kompetenzniveau

NUTZER-GRUPPE	PRIVAT-HEITS-/ KONTROLL-BEDÜRFNIS	KOMPETENZ-NIVEAU	GRAD AN SORGE BEZÜGLICH INTERNET
Digital Natives	niedrig	hoch	gelassen
Technikaffine	hoch	hoch	mittleres Niveau
Technik-distanzierte	hoch	niedrig	ausgeprägte Sorge

Gleichzeitig herrscht bei allen Nutzern dahingehend Einigkeit, dass die Nutzung des Internets aufgrund der hohen technischen Komplexität bis zu einem gewissen Grad mit einem Kontrollverlust einhergeht. Es ist also kaum verwunderlich, dass der Kontrollverlust bei der Internetnutzung auch als Verlust an Privatheit – eben an Kontrollmöglichkeiten – wahrgenommen wird.

Die verschiedenen Gruppen gehen mit diesem Kontrollverlust also *auf verschiedene Weise* um – *sie alle* gehen aber damit um. Eben darin besteht die gleichzeitige Abweichung und Identität der Nutzerperspektiven. Bestätigung erfährt der gefühlte Kontrollverlust durch die Diagnose der Experten. Man mag die aktuellen Transformationsprozesse als harmlos oder dramatisch einschätzen, die soziale Frage,

die sich stellt, ist jedoch nicht von der Hand zu weisen. Beispielsweise ließe sich der Standpunkt einnehmen, dass den Nutzern durch das Sammeln der Daten seitens der Betreiber in den seltensten Fällen ein individuell spürbarer Schaden entsteht; vielmehr werden die Nutzer nur mit gezielt auf ihr Profil zugeschnittener Werbung konfrontiert. Aus dieser Perspektive werden also lediglich ihre Wünsche besser bedient. Die soziale Frage, die sich damit stellt, lautet jedoch, ob wir tatsächlich soziale Formen entwickeln wollen, die von einem solchen Wünsche-Paternalismus charakterisiert sind: Welche Mentalität entwickelt sich in Gemeinwesen, in denen den Akteuren die Wünsche von den Lippen abgelesen werden, noch bevor sie diesen zu Bewusstsein kommen?[166] Wollen wir das?

Weitere Fragen schließen sich an. Wenn Nutzer beispielsweise den AGBs bestimmter E-Mail-Provider zustimmen, treten sie diesen damit das Recht ab, die per E-Mail gesendeten Informationen auszuwerten. Tauschen die Akteure dienstliche Informationen aus, so treten sie diese unberechtigterweise dem Provider ab. Nun nutzen die Provider den Zugriff auf diese Daten zumindest nicht offen aus, im Resultat passiert also gar nichts. Die soziale Frage wäre, ob uns das reicht: Aufgeklärte Monarchen foltern ihre Untertanen nicht, demokratischen Gemeinwesen reicht es aber nicht, dass dies empirisch nicht geschieht: Unterbunden wird schon die *Möglichkeit* der Folterung.

Das zuletzt angeführte, reichlich drastische Beispiel soll nun keineswegs dem Zweck dienen, die Problematik mit zusätzlicher Dramatik aufzuladen, geht es uns hier doch um eine möglichst nüchterne Analyse. Was diese in erster Linie zutage fördert, ist, dass die genannten sozialen Fragen aufgrund der offenkundig bestehenden Asymmetrien von vielen Nutzern *gar nicht erst gestellt werden können*. Nichtsdestotrotz haben die wiederholt geäußerten Befürchtungen und Wünsche der Nutzer es uns zunächst ermöglicht zu abstrahieren, bezüglich welcher Praktiken sie einen Kontrollverlust genau fürchten (beziehungsweise sich mehr Kontrolle wünschen). Wir werden die in den obigen Zusammenfassungen verstreut vorliegenden Befürchtungen und Wünsche nun vor Hintergrund der Expertenperspektive in konkrete praktische Vorschläge überführen. Diese dienen erstens dem Zweck, den Nutzern die Bedingungen, unter denen sie agieren sichtbar zu machen; zweitens sollen sie stärker in die Lage versetzt werden, über einen höheren Grad an Kontrolle zu verfügen – und zwar an den Stellen, an denen ihnen diese wichtig ist.

1.7 SCHLUSS: FAIRE INFORMATIONSPRAKTIKEN – ODER: ZEHN VORSCHLÄGE ZUR ENTWICKLUNG EINER KULTUR DER PRIVATSPHÄRE

Eine Möglichkeit, persönliche Informationen individuell kontrollieren zu können, wird in der Ausbildung einer fairen Informationspraxis gesehen. Letztere kann wiederum nur *kollektiv* erzeugt werden – wir haben darauf im Textverlauf (unter Bezug auf Paul Dourish und Ken Anderson) mehrfach hingewiesen. Eine Kultur der Privatsphäre und des Vertrauens bildet ihrerseits die Grundlage einer solchen Informationspraxis. Ein leicht nachvollziehbares Beispiel dafür stellt die Einspeisung von persönlichen Informationen durch Dritte (zum Beispiel Fotos) dar: Während das Problem technisch von vornherein schwerlich zu lösen sein dürfte, ist es zwar denkbar, dass Gesetze erlassen werden, die eine solche Praxis verbieten. Dass ein gesetzliches Verbot in der Praxis umzusetzen wäre, ist aber wenig wahrscheinlich: Sollten tatsächlich Gerichte mit Klagen wegen der Einstellung der berühmten Partyfotos behelligt werden? Da eine solche Praxis für die Nutzer dennoch ein Problem darstellt, scheinen kollektive Normen, die solche Praktiken sozial sanktionieren, am besten geeignet.

Eine Kultur der Privatsphäre und des Vertrauens zur Formung einer fairen Informationspraxis kann sich indes nur dann

[166] So zitiert Hof Facebook's Chief Operations Officer Sheryl Sandberg mit den Worten: „We're not really demand fulfillment, when you've already figured out what you're going to buy [...] We're demand generation, before you know you want something." Vgl. Hof 2011, S. 67.

etablieren, wenn ein hinreichend weitverbreitetes Verständnis des Internet als öffentliches, kollektives Gut besteht, für dessen Erhalt alle Beteiligten Verantwortung tragen. Gleichzeitig kann den Nutzern diese Verantwortung nur dann aufgebürdet werden, wenn diese über ausreichend hohe Kompetenzen und Entscheidungsmöglichkeiten verfügen. Wie oben dargestellt, perspektivieren die Digital Natives *Internet Privacy* tendenziell als individuelles Problem und sehen Gefährdungen ihrer Privatheit vor allem durch andere Nutzer. Bei den anderen Nutzergruppen verschiebt sich der Blick dann immer weiter hin zu den Betreibern: Die Technikaffinen nehmen andere Nutzer und Betreiber gleichermaßen in den Blick, bei den Technikdistanzierten erfolgt eine weitere Verschiebung hin zum Fokus auf die Betreiber. Dass die beiden letzteren Gruppen auch den ungebetenen *Erhalt* von Informationen als Privatheitsbruch bestimmen, ist dem Umstand geschuldet, dass sie den Praktiken der Betreiber viel größeren Raum in ihren Überlegungen geben, und dass sie diese Praktiken wiederum als Teil eines gesellschaftlichen Zusammenhangs verstehen. Der Individualismus der Digital Natives führt hingegen dazu, dass sie zum Beispiel die Möglichkeiten aus dem Blick verlieren, durch statistische Korrelation großer Datenmengen auch dann identifizierbar zu werden, wenn sie individuell nur reduziert persönliche Informationen ins Internet einspeisen. Jeder Nutzer, der einige – für sich genommen: unschuldige – Klicks tätigt, trägt mit anderen Worten Verantwortung für alle anderen, für das kollektive Gut des Internets. Der Zusammenhang zwischen mikrologischem Verhalten und dem emergenten makrologischen Effekt ist jedoch ähnlich schwer wahrnehmbar wie beispielsweise beim Klimawandel.

Die Nutzer selbst äußern indes wiederholt den Wunsch nach mehr Wissen und Kompetenz in Bezug auf solcherlei Zusammenhänge. Es geht uns hier also in keiner Weise um Nutzerschelte, sondern um den Vorschlag von Maßnahmen, die geeignet wären, den Wünschen der Nutzer aus unserer Sicht nachzukommen. Bevor wir unseren Durchgang beginnen, wollen wir vorausschicken, dass keineswegs alle Nutzer ihre Privatheit im Internet an allen genannten Stellen gleichermaßen gefährdet sehen. Unsere Vorschläge sollten daher als Versuch verstanden werden, die Wahlmöglichkeiten jedes einzelnen Nutzers zu vergrößern. Im Übrigen stellt keine der nun folgenden zehn Maßnahmen eine hinreichende Bedingung zur Herstellung fairer Informationspraktiken dar.

Als erstes Problem ist ohne jeden Zweifel die mangelnde Transparenz der Betreiberpraktiken anzugehen. Während die Praktiken der Nutzer für viele Betreiber äußerst genau zu beobachten sind, gilt das Gegenteil keineswegs. Die Nutzer wissen weder, welche ihrer persönlichen Information wo und wie lange gespeichert, noch wie diese weiterverarbeitet und ob und an wen sie weitergegeben werden. Die Situation trägt die Grundzüge dessen, was Michel Foucault[167] einst am Modell des Panoptikums beschrieb:

> *„The panopticon is the name given by Jeremy Bentham to the design for a prison that would facilitate the efficient observation or surveillance of prisoners by guards or supervisors who might periodically occupy a central tower. [...] The panoptic technology was not limited to surveillance alone but included the classification and isolation of subjects by category or type. Once divided, a panoptic structure could be used as a ‚laboratory'; it could be used as a machine to carry out experiments, to alter behavior, to train or correct individuals."*[168]

Diesen Gedanken aufgreifend, spricht Helen Nissenbaum von der drohenden Gefahr eines „informational panopticon."[169] Entscheidendes Charakteristikum des Panoptikums ist die Tatsache, dass die Beobachteten die Beobachter selbst nicht wahrnehmen können, in der Folge also nie wissen, ob sie beobachtet werden. Die Beobachteten passen

[167] Vgl. Foucault 1976.
[168] Gandy 1993, S. 9.
[169] Nissenbaum 2010, S. 75.

daher ihr Verhalten in einer Art vorauseilendem Gehorsam an die vermuteten Wünsche der Beobachter an. Während normative Privatheitstheorien in solchen Verhaltensanpassungen erhebliche Gefahren für demokratisch organisierte Gemeinwesen sehen, spielt es für unsere Argumentation nur eine untergeordnete Rolle, ob die befürchtete Verhaltensanpassung im Internet empirisch auftritt oder nicht. Es entspricht schlicht und ergreifend keiner fairen Informationspraxis, wenn die Nutzerpraktiken von den Betreibern beobachtet werden können, die Praktiken letzterer für erstere aber gänzlich intransparent bleiben. Unser *erster* Vorschlag besteht daher darin, dass Nutzer zumindest grundsätzlich Aufschluss darüber erhalten, wenn ihre Informationen gespeichert werden, wenn (und wie) sie weiterverarbeitet und an wen sie weitergegeben werden. Und es reicht keineswegs aus, solche Benachrichtigungen auf grundsätzliche Erklärungen in überbordenden und unverständlichen AGBs zu beschränken, die zu lesen ohnehin niemand die Zeit hat. Stattdessen wären konkrete Angaben über tatsächlich erfolgende Datenverarbeitungen angebracht. Gefragt wären hier die Betreiber selbst als wirtschaftliche Akteure sowie die Rechtsprechung als Rahmen setzende Instanz wirtschaftlicher Aktivitäten.

Damit kommen wir zum *zweiten Punkt*, und hier können wir es kurz machen: Es ist allgemein bekannt, dass die AGBs sehr vieler Websites zu lang, zu unübersichtlich und zu unverständlich sind. Nutzer haben weder die Zeit noch das juristische Grundverständnis, um diese rezipieren oder gar verstehen zu können. Das führt dazu, dass sie allzu oft die Bedingungen nicht kennen, unter denen sie eine bestimmte Anwendung nutzen. Dass die Betreiber die AGBs darlegen müssen, ist zwar angemessen, doch führt dies aus den genannten Gründen in der Praxis keineswegs dazu, dass die „information asymmetry"[170] durchbrochen wird. Im Rahmen unserer Untersuchung äußerste ein Nutzer den Wunsch nach der Entwicklung von Standard-AGBs, die für bestimmte Anwendungen im Internet grundsätzlich gelten sollten; wir schließen uns dem Vorschlag an und fügen hinzu, dass diese AGBs im Rahmen von Medienunterricht in der Schule gelehrt werden könnten (mehr dazu weiter unten) und dass die Betreiber verpflichtet sein sollten, eventuelle Abweichungen von den Standard-AGBs im Internet aufzuführen. Auf diese Weise würden die Nutzer die grundsätzlichen Normalbedingungen kennen, unter denen sie eine Anwendung nutzen, und sich zudem sehr schnell einen Überblick über Abweichungen von diesen Bedingungen verschaffen können. Alternativ wäre auch die maschinelle Auslesung von AGBs denkbar, die den Nutzern die Nutzungsbedingungen leicht verständlich darstellt. Technische Standardisierungslösungen existieren ja bereits (P3P etc.), deren Verbreitung wäre zu fördern.

Das Transparenzproblem liegt *drittens* in den praktisch mangelhaften Kontrollmöglichkeiten der Nutzer begründet, die Speicherung, Weiterverarbeitung und Weitergabe persönlicher Informationen zu kontrollieren. Selbst wenn die Nutzer die in den AGBs vieler Betreiber zu findenden diesbezüglichen Angaben verstehen könnten, bliebe ihnen mit diesem Wissen nicht viel mehr, als nach dem Prinzip „take it or leave it" zu verfahren. Wünschenswert wäre in dieser Hinsicht also ein Opt-In-Prinzip, das den Nutzern eine wirklich Wahl ließe, indem sie zum einen von den Betreibern aktiv über deren Praktiken informiert würden und indem sie zum anderen eine Anwendung auch dann nutzen könnten, wenn sie der Speicherung, Weiterverarbeitung und Weitergabe ihrer Informationen *nicht* zustimmen würden. Hier wären somit der Erlass von Gesetzen und die Rechtsprechung gefragt, und die Bemühungen, die die EU-Kommissarin für Justiz, Grundrechte und Bürgerschaft Viviane Reding im Zuge der EU-Datenschutznovelle Anfang 2012 vorgestellt hat, gehen offensichtlich auch genau in diese Richtung.

Eine *vierte* Schwierigkeit zur Lösung des Transparenzproblems stellt sich durch deren gefühlte Unerreichbarkeit der Betreiber ein. An diesem Punkt zeigt sich deutlich, zu welch hohem Lern- und Abstraktionsaufwand die Nutzer gezwungen sind, um mit den neuen Verhältnissen umzugehen.

[170] Im Sinne von Acquisti / Grossklags 2005.

Historisch betrachtet, zwang schon die Ausbildung bürokratischer Institutionen die Akteure zur Interaktion mit abstrakten Strukturen, doch wurde diesen Strukturen durch Beamte und Büros zumindest noch eine Repräsentanz im physischen Raum gegeben. Mit der Virtualisierung erhält die Abstraktionstendenz eine neue Dynamik. Die Inanspruchnahme von Dienstleistungen durch virtuelle Dienstleister wird folgerichtig fast durchweg als Überforderung angesehen. Die Schaffung von Repräsentanzen („Filialen") der Betreiber im physischen Raum – inklusive ansprechbarer Personen (Vertreter der Betreiber), bei denen im Zweifelsfall die Wahrung von Normen eingefordert werden kann, würde zweifellos das Vertrauen der Nutzer in die genutzten Anwendungen maßgeblich erhöhen. Hier wären aber die wirtschaftlichen Akteure selbst gefragt, und angesichts der mit der Einrichtung solcher Repräsentanzen verbundenen Kosten und des harten Verdrängungswettbewerbs im Internet scheint es mehr als fraglich, ob es dazu kommt.

Als zweitbeste Lösung bietet sich *fünftens* die Einrichtung einer weithin wahrnehmbaren Zertifizierungsinstanz an, eine Art Stiftung Warentest für *Internet Privacy*. Eine Vertrauensprüfung des technisch-virtuellen Gegenübers erscheint den Nutzern mitunter unmöglich, das Gegenüber bleibt anonym. Eine Delegation der Vertrauensprüfung an eine unabhängige Instanz, die nicht nur die technische und ökonomische Sicherheit des Interaktionspartners bestimmt, sondern auch die Wahrung von Privatheitsansprüchen könnte das Problem zumindest verringern.

Zuständig für die Einrichtung einer solchen Instanz wäre die Politik (die Stiftung Warentest arbeitet ja in staatlichem Auftrag), und auch unser *sechster* Vorschlag nimmt die Politik in die Pflicht. Gerade technikdistanzierte Nutzer sehen sich nicht nur mit der technischen Komplexität Internet basierter Transaktionen überfordert, sondern auch mit dem rasanten *Wandel* technischer Möglichkeiten und Anforderungen. Nicht nur, aber vor allem für diese Nutzergruppe böte sich die Einrichtung von Trust Centern an, welche die persönlichen Informationen der Nutzer treuhänderisch verwalten. Letztere könnten die Bedingungen ihrer Transaktionen gemäß ihren Privatheitsvorstellungen in regelmäßigen Abständen justieren, dem Trust Center obläge es dann, demgemäß die Transaktionen im Internet abzuwickeln.

Eine vollständige Delegation der Verantwortung ist gleichwohl undenkbar, auch die Nutzer selbst müssen ihren Teil zur Entwicklung fairer Informationspraktiken beitragen. Unser *siebter* Vorschlag bezieht sich denn auch auf die Nutzer, oder genauer: Auf das oben angesprochene Problem eines stärkeren Bewusstseins für die gesellschaftliche Dimension von *Internet Privacy*. Dass die eigenen Aktivitäten die Privatheit anderer Nutzer betrifft – beispielsweise dann, wenn Fotos eingestellt werden und dergleichen – scheint bislang nur bedingt reflektiert zu werden. Zu überlegen wäre hier zum einen, wie ein gesamtgesellschaftlicher Diskurs zur Thematik grundsätzlich in Gang gebracht werden könnte. Einer der Orte, an dem dies erfolgen könnte, wären zum Beispiel die Schulen. An vielen Punkten unserer Untersuchung artikuliert sich die Notwendigkeit der Entwicklung eines eigenständigen Faches Medienkunde. Ein solches Fach könnte den dringend benötigten zeitlichen Raum bieten, um über die Auseinandersetzung mit der Problematik ein kollektives Bewusstsein zu schaffen, um Spielregeln – das heißt Normen – für einen angemessenen Umgang miteinander auszuhandeln und um die technische und rechtliche Grundkompetenz heutiger und zukünftiger Generationen auszubilden. Es ginge dabei nicht um Frontalpädagogik oder Benotung – das wäre angesichts der oftmals hohen Schüler- und niedrigen Lehrerkompetenzen ohnehin fragwürdig; sinnvoll wäre vielmehr ein Freiraum für Diskussionen und die Weitergabe von Anwendungswissen. (Wie funktioniert das Internet in groben Zügen? Wem gehören die Daten? Was kann man mit ihnen alles machen? Aber auch: welche Auswirkungen haben welche Praktiken auf meine Mitmenschen? Wie funktionieren die Privatheitseinstellungen auf SNS-XY? Wie kann ich anonym surfen? usw.). Reflektierte und kompetente Nutzer können

die Punkte identifizieren, an denen sie Kontrolle über ihre persönlichen Informationen ausüben wollen. Ein Großteil des derzeitigen Problems besteht darin, dass dies gerade nicht der Fall ist. Die Betreiber wissen viel, die Nutzer wenig. Letztere können bestimmte Wünsche gar nicht äußern, weil sie die Bedingungen und Möglichkeiten nicht kennen, unter denen sie agieren.

Per Bewusstseinsschaffung, Normenerfindung und Vermittlung von Anwendungswissen wären die menschlichen Operationsketten mit Sicherheit besser in der von den Nutzern gewünschten Weise zu formen. Wissen, wie die angestrebte Kontrolle zu erlangen wäre, ist aber nur dann hilfreich, wenn auch die technischen Operationsketten im Sinne der Nutzer zu formen sind. Hierzu unterbreiten wir abschließend einige Vorschläge.

Unser *achter* Vorschlag betrifft das Problem der ungewollten Erstellung von Profilen in Bezug auf das Suchverhalten. Aufseiten der Nutzer besteht mitunter der Wunsch, keine Profile für die Platzierung von Profilwerbung liefern zu müssen. Dahinter steht die Befürchtung, dass sich aus der Kombination verschiedener Suchanfragen ein Profil der Wünsche, Vorlieben und Interessen erstellen lässt. Wenn es möglich wäre, die verschiedenen Suchvorgänge aufzusplitten, wäre ein Teil des Problems zumindest abgeschwächt. Denkbar wäre, dass Nutzer eine Suchidentität für Bücher, eine für Musik, eine für Autovermietungen verwenden können, ohne dass diese zusammengeführt werden (können). Oder dass eine Suchidentität für Studienzwecke, eine für Urlaubsvorbereitungen, eine zur Unterhaltung verwendet werden kann. Auf diese Weise würden die Nutzer den ausdrücklich geschätzten praktischen Vorzug der Archivierung des Suchverlaufs weiterhin genießen können, die verschiedenen Teilaspekte ihrer Persönlichkeit wären aber nicht zu kombinieren, sodass sich seitens der Betreiber ein weniger umfassendes Bild der Nutzer ergeben würde.

Genau wie der vorherige richtet sich auch unser *neunter* Vorschlag an die Informatik und auch dieser betrifft die Profilbildung, bietet allerdings nur eine Teillösung. Viele Nutzer lehnen die Archivierung ihrer Such- und Kaufgeschichte ab, welche bei der Nutzung von eCommerce-Diensten entsteht. Um zumindest die Suchhistorie unsichtbar zu machen, wäre die Entwicklung einer Software vorstellbar, die den Anbieter nach dem Zufallsprinzip mit beliebigen Suchanfragen bombardiert. Das Suchprofil wäre damit unkenntlich gemacht (das Kaufverhalten allerdings nach wie vor nicht verschleiert).

Der letzte und *zehnte* Vorschlag betrifft die ungewollte Verlinkung persönlicher Informationen. Nutzer beklagen zum Beispiel immer wieder, dass Informationen über ihre Freizeitaktivitäten über Suchmaschinen im Internet und damit für ihre Kollegen oder Arbeitgeber auffindbar sind. Hier wäre die Frage, ob und wie eine von den Nutzern bestimmte „Ent-Linkung" zu bewerkstelligen sein könnte, ähnlich dem Außer-Kraft-Setzen der Suche nach Profilen auf SNS über viel genutzte Suchmaschinen. Hier unsere zehn Vorschläge noch einmal in tabellarischer Form:

Tabelle 2: Zehn Vorschläge zur Entwicklung einer Kultur der Privatsphäre

VORSCHLAG	PROBLEM	LÖSUNG	ZUSTÄNDIGKEIT	MASSNAHME
1	Mangelnde Transparenz der Betreiberpraktiken	Praktiken sichtbar machen	Wirtschaft/Recht	Benachrichtigung bzgl. Speicherung/Verarbeitung/ Weitergabe
2	Unverständliche AGBs	Entwicklung von Standard-AGBs // AGB-Auslesetool	Recht // Informatik	Erlass von Gesetzen // Software-Entwicklung
3	Ungewollte Speicherung/ Verarbeitung/Löschung	Rechtliche Verankerung eines Opt-In-Verfahrens bzgl. dieser Praktiken	Recht	Erlass von Gesetzen (s. EU-Datenschutznovelle)
4	Unerreichbarkeit der Betreiber	Real World Repräsentanzen	Wirtschaft	Dependancen eröffnen
5	Vertrauensprüfung Nutzern nicht möglich	Delegation an Zertifizierungsinstanz	Politik (Wirtschaft)	Stiftung Warentest für *Internet Privacy*
6	Andauernder techn. Wandel überfordert Nutzer	Delegation an TrustCenter	Politik	Einrichtung von Trust Centern
7	Mangelndes Bewusstsein bzgl. gesellschaftlicher Dimension // Einspeisung von Informationen durch Dritte // Mangelnde Medienkompetenz (Technik, Rechtslage)	Bewusstseinsschaffung // Normenaushandlung // Kompetenzerzeugung	Politik, Medien, Praxis, Pädagogik	Medialer Diskurs, Unterricht
8	Ungewollte Erstellung von Profilen bzgl. Suchverhalten / Suchmaschinen	Aufsplittung der Such-aktivitäten nach Bereichen	Informatik	Software-Entwicklung
9	Ungewollte Erstellung von Profilen / eCommerce	Bombardierung von Suchmaschinen mit Zufallsanfragen	Informatik	Software-Entwicklung
10	Verlinkung von in unterschiedlichen Kontexten eingespeisten Informationen	Ent-Linkung	Informatik	Tool

Wie zu sehen, fördert unsere Untersuchung eine ganze Reihe möglicher Anstrengungen zutage, die von unterschiedlichen akademischen Disziplinen und gesellschaftlichen Feldern in Angriff genommen werden müssten. Aufgrund der Heterogenität der Problematiken können wir nicht für jeden einzelnen Vorschlag angeben, ob dieser umsetzbar oder praktikabel wäre. Die wichtigste Voraussetzung für eine Kultur der Privatsphäre und des Vertrauens im Internet scheint uns daher die andauernde interdisziplinäre Erforschung und gesellschaftliche Auseinandersetzung mit den sich immer wieder neu stellenden Problemen.

LITERATUR

Acquisti / Grossklags 2003
Acquisti, A. / Grossklags, J.: *Losses, Gains and Hyperbolic Discounting: An Experimental Approach to Information Security Attitudes and Behaviour*. URL: http://www.cpppe.umd.edu/rhsmith3/papers/Final_session6_acquisti.grossklags.pdf [Stand: 29.02.12].

Acquisti / Grossklags 2005
Acquisti, A. / Grossklags, J.: „Privacy and Rationality in Individual Decision Making." In: *IEEE Computer Society 3*, Nr. 1, 2005, S. 26-33.

Akrich 1992
Akrich, M.: „The De-Scription of Technological Objects." In: Bijker, Wiebe E./Law, John (Hrsg.): *Shaping Technology/Building Society. Studies in Sociotechnical Change*, Cambridge, Mass.: MIT Press 1992.

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

Altman 1977
Altman, I.: „Privacy Regulation: Culturally Universal or Culturally Specific?" In: *Journal of Social Issues 33*, Nr. 3 (1977), S. 67-83.

Arendt 1951
Arendt, H.: *The Origins of Totalitarianism*, New York: Harcourt, Brace 1951.

Bailey 2000
Bailey, J.: „Some Meanings of ‚the Private' in Sociological Thought." In: *Sociology 34*, Nr. 3, 2000, S. 381-401.

Bauer 2006
Bauer, J.: *Warum ich fühle, was du fühlst. Intuitive Kommunikation und das Geheimnis der Spiegelneurone*, Hamburg: Hoffmann und Campe 2006.

Bernsdorf 1969
Bernsdorf, W. (Hrsg.): *Wörterbuch der Soziologie, 2. Auflage*, Stuttgart: Enke 1969.

Bijker / Law 1992
Bijker, W. E. / Law, J. (Hrsg.): *Shaping Technology/Building Society. Studies in Sociotechnical Change*, Cambridge, Mass.: MIT Press 1992.

BITKOM 2011
BTKOM: *Soziale Netzwerke. Eine repräsentative Untersuchung zur Nutzung sozialer Netzwerke im Internet*. URL: http://www.bitkom.org/files/documents/BITKOM_Publikation_Soziale_Netzwerke.pdf [Stand: 14.01.12].

Boudon / Bourricaud 1989
Boudon, R. / Bourricaud, F.: *A Critical Dictionary of Sociology*, London u. a.: Routledge 1989.

boyd 2008
boyd, danah: „Facebook's Privacy Trainwreck. Exposure, Invasion, and Social Convergence." In: Convergence: *The International Journal of Research into New Media Technologies 14*, Nr. 1 (2008), S. 13-20.

DIVSI 2012
Deutsches Institut für Vertrauen und Sicherheit im Internet (DIVSI): *DIVSI Milieu-Studie zu Vertrauen und Sicherheit im Internet*. URL: https://www.divsi.de/sites/default/files/presse/docs/DIVSI-Milieu-Studie_Gesamtfassung.pdf [Stand: 01.03.12].

Dourish / Anderson 2006
Dourish, P./Anderson, K.: „Collective Information Practice: Exploring Privacy and Security as Social and Cultural Phenomena." In: *HUMAN-COMPUTER INTERACTION 21* (2006), S. 319-342.

Dörflinger 2009
Dörflinger, T.: *Das Private auf dem globalen Präsentierteller. Chancen und Risiken moderner Kommunkationstechnologie aus Sicht deutscher Bürger*, Münster: LIT-Verlag 2009.

Endruweit / Trommsdorf 1989
Endruweit, G. / Trommsdorff, G. (Hrsg.): *Wörterbuch der Soziologie*, Stuttgart: Lucius & Lucius 1989.

Endruweit / Trommsdorf 2001
Endruweit, G. / Trommsdorff, G. (Hrsg.): *Wörterbuch der Soziologie, 2. Auflage.* Völlig überarbeitete Gesamtausgabe, Stuttgart: Lucius & Lucius 2001.

Flanagan / Howe / Nissenbaum 2008
Flanagan, M. / Howe, D. C. / Nissenbaum, H.: „Embodying Values in Technology. Theory and Practive." In: van den Hoven, J./Weckert, J. (Hrsg.): *Information Technology and Moral Philosophy*, Cambridge, UK: Cambridge University Press 2008, S. 322-353.

Foucault 1976
Foucault, M.: *Überwachen und Strafen. Die Geburt des Gefängnisses*, Frankfurt/M.: Suhrkamp 1976.

Ganascia 2010
Ganascia, J.-G.: „The Generalized Sousveillance Society." In: *Social Science Information 49*, Nr. 3 (2010), S. 1-19.

Gandy 1993
Gandy, O.: *The Panoptic Sort. A Political Economy of Personal Information*, Boulder, CO: Westview Press 1993.

Giddens 1995
Giddens, A.: *Konsequenzen der Moderne*, Frankfurt/M.: Suhrkamp 1995.

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

Habermas 1962
Habermas, J.: *Strukturwandel der Öffentlichkeit. Untersuchungen zu einer Kategorie der bürgerlichen Gesellschaft*, Neuwied: Luchterhand 1962.

Heller 2011
Heller, C.: *Post-Privacy. Prima Leben ohne Privatsphäre*, München: C.H.Beck 2011.

Hillmann 2007
Hillmann, K.-H.: *Wörterbuch der Soziologie*, Stuttgart: Kroener 2007.

Hodel / Schütte / Biedermann 2008
Hodel, T. B./Schütte, A./Biedermann, M.: „Privacy in Tomorrow's Internet." In: Myrach, T./Zwahlen, S. M. (Hrsg.): *Virtuelle Welten? Die Realität des Internets*, Bern: Peter Lange Verlag, 2008, S. 259-278.

Hof 2011
Hof, R. D.: „You Are the Ad. " In: *Technology Review* (Mai/Juni 2011). URL: http://www.technologyreview.com/web/37334/ [Stand 29.05.12].

Introna 1997
Introna, L.: „Privacy and the Computer: Why We Need Privacy in the Information Society." In: *Metaphilosophy 28*, Nr. 3, 1997, S. 259-275.

Jary / Jary 1991
Jary, D. / Jary, J.: *Collins Dictionary of Sociology*, New York u. a.: Harper Collins 1991.

Knorr-Cetina 1998
Knorr-Cetina, K.: „Sozialität mit Objekten: Soziale Beziehungen in post-traditionalen Wissensgesellschaften. " In: Rammert, W. (Hrsg.): *Technik und Sozialtheorie*, Frankfurt/M. und New York: Campus 1998, S. 83-120.

Köhntopp / Köhntopp / Seeger 1997
Köhntopp, K. / Köhntopp, M. / Seeger, M.: Sperrungen im Internet. Eine systematische Aufarbeitung der Zensurdiskussion. URL: http://kris.koehntopp.de/artikel/blocking/ [Stand 28.02.12].

Kurz / Rieger 2011
Kurz, C. / Rieger, F.: *Die Datenfresser. Wie Internetfirmen und Staat sich unsere persönlichen Daten einverleiben und wie wir die Kontrolle darüber zurückerlangen*, Frankfurt/M.: S. Fischer2011.

Krueger / Casey 2009
Krueger, R. A. / Casey, M. A.: *Focus Groups (4th Edition). A Practical Guide for Applied Research*, Los Angeles et al.: Sage Publications 2009.

Latour 1992
Latour, B.: „Where Are the Missing Masses? The Sociology of a Few Mundane Artifacts." In: Bijker, W. E./Law, J. (Hrsg.): *Shaping Technology/Building Society. Studies in Sociotechnical Change*, Cambridge, Mass.: MIT Press 1992, S. 225-258.

Leroi-Gourhan 1987
Leroi-Gourhan, A.: *Hand und Wort. Die Evolution von Technik, Sprache und Kunst*, Frankfurt/M.: Suhrkamp 1987.

Luhmann 2000
Luhmann, N.: *Vertrauen: Ein Mechanismus der Reduktion sozialer Komplexität*, Stuttgart: UTB 2000.

Margulis 2003a
Margulis, S.: „Privacy as Social Issue and Behavioral Concept." In: *Journal of Social Issues 59*, Nr. 2, 2003, S. 243-261.

Margulis 2003b
Margulis, S.: „On the Status and Contribution of Westin's and Altman's Theories of Privacy." In: *Journal of Social Issues 59*, Nr. 2, 2003, S. 411-430.

Marx 1994
Marx, G. T.: *New Telecommunications Technologies And Emergent Norms*. URL: http://web.mit.edu/gtmarx/www/telecom.html [Stand 12.01.12].

Marx 2001
Marx, G. T.: „Murky Conceptual Waters: The Public and the Private." In: *Ethics and Information Technology 3*, 2001, S. 157-169.

Marx / Muschert 2007
Marx, G. T. / Muschert, G. W.: „Personal Information, Borders, and the New Surveillance Studies." In: *Annual Review of Law & Social Science 3*, 2007, S. 375-395.

Marx / Muschert 2009
Marx, G. T. / Muschert, G. W.: „Simmel on Secrecy. A Legacy and Inheritance for the Sociology of Information." In: Papiloud, C./Rol, C. (Hrsg.): *Soziologie als Möglichkeit. 100 Jahre Georg Simmels Untersuchungen über die Formen der Vergesellschaftung*, Wiesbaden: VS Verlag für Sozialwissenschaften 2009, S. 217-236.

Mayring 2008
Mayring, P.: *Qualitative Inhaltsanalyse: Grundlage und Techniken (10. Auflage)*, Weinheim: Beltz 2008.

Meyrowitz 2002
Meyrowitz, J.: „Post-Privacy-America." In: Weiß, R./Groebel, J. (Hrsg.): *Privatheit im öffentlichen Raum. Medienhandeln zwischen Individualisierung und Entgrenzung*, Opladen: Leske und Budrich 2002, S. 153-205.

Nissenbaum 2010
Nissenbaum, H.: *Privacy in Context*. Technology, Policy, and the Integrity of Social Life, Standford, California: Stanford University Press 2010.

Regan 1995
Regan, P. M.: *Legislating Privacy. Technology, Social Values, and Public Policy*, Capel Hill & London: University of North Carolina Press 1995.

Reinecke / Trepte 2008
Reinecke, L./Trepte, S.: „Privatsphäre 2.0: Konzept von Privatheit, Intimsphäre und Werten im Umgang mit ‚user-generated-content'." In: Zerfaß, A./Welker, M./Schmidt, J. (Hrsg.): *Kommunikation, Partizipation und Wirkungen im Social Web. Band 1: Grundlagen und Methoden: Von der Gesellschaft zum Individuum*. Köln: Herbert von Harlem Verlag 2008, S. 205-228.

Reinhold / Lamnek / Recker 2000
Reinhold, G./Lamnek, S./Recker, H.: *Soziologie-Lexikon*, München/Wien: Oldenbourg 2000.

Ritzer 2007
Ritzer, G. (Hrsg.): *The Blackwell Encyclopedia of Sociology*, Malden, Mass.: Blackwell 2007.

Rössler 2001
Rössler, B.: *Der Wert des Privaten*, Frankfurt/M.: Suhrkamp 2001.

Sassen 2004
Sassen, S.: „Towards a Sociology of Information Technology." In: *Current Sociology 50*, Nr. 3, 2002, S. 365-388.

Schneier 2010
Schneier, B.: *Google and Facebook's Privacy Illusion: These companies and others say privacy erosion is inevitable – but they're making it so*. URL: http://www.schneier.com/essay-311.html [Stand: 12.01.12].

Sennett 1983
Sennett, R.: *Verfall und Ende des öffentlichen Lebens. Die Tyrannei der Intimität*, Frankfurt/M.: S. Fischer 1983.

Simmel 1992
Simmel, G.: „Das Geheimnis und die geheime Gesellschaft". In: Ders.: *Georg Simmel Gesamtausgabe Band 11, Soziologie: Untersuchungen über die Formen der Vergesellschaftung*, Frankfurt/M.: Suhrkamp 1992, S. 383-455.

Solove 2008
Solove, D. J.: *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.

Spectra 2011
Spectra: *Nervige Handys in der Öffentlichkeit – rücksichtsvolle Nutzung nimmt aber leicht zu*. URL: http://www.spectra.at/archiv/Aktuell_07_11_Handynutzung.pdf [Stand: 12.01.2012].

Steeves 2009
Steeves, V.: „Reclaiming the Social Value of Privacy." In: Kerr, I./Lucock, C./Steeves, V. (Hrsg.): *Lessons from the Identitiy Trail: Anonymity, Privacy and Identity in a Networked Society*, Oxford, UK: Oxford University Press 2009, S. 191-208.

Strum / Latour 1987
Strum, S./Latour, B.: "Redefining the Social Link: From Baboons to Humans." In: *Social Science Information 26* (1987), S. 783-802.

Sultan / Urban / Shankar / Bart 2002
Sultan, F./Urban, G.L./Shankar, V./Bart, Y. (2002): *Determinants and Role of Trust in E-Business: A Large Scale Empirical Study. MIT Sloan Working Paper No. 4282-02*. URL: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=380404 [Stand: 14.01.12].

Turner 2006
Turner, B. S. (Hrsg.): *Cambridge Dictionary of Sociology*, Cambridge, UK: Cambridge University Press 2006.

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

2 IT AND PRIVACY FROM AN ETHICAL PERSPECTIVE DIGITAL WHONESS: IDENTITY, PRIVACY AND FREEDOM IN THE CYBERWORLD[171]

RAFAEL CAPURRO, MICHAEL ELDRED, DANIEL NAGEL

ABSTRACT

The *first aim*, employing the phenomenological method, is to provide well-articulated concepts by thinking through elementary phenomena of today's world, focusing on *privacy* and the *digital*, to clarify *who* we are in the cyberworld — hence a phenomenology of *digital whoness*. The *second aim*, employing the hermeneutic method, is to engage critically with older and current literature on privacy, including in today's emerging cyberworld, whose most important results are the critique of merely *informational* privacy as well as of the *autonomous subject* vis-à-vis an *objective, reified* world, as opposed to a self engaged in ongoing social power-plays. Phenomenological results include concepts of i) *self-identity* through *interplay* with the world, ii) *personal privacy* in contradistinction to the *privacy of private property*, iii) the *cyberworld* as an artificial, digital dimension in order to discuss iv) what *freedom* in the cyberworld can mean, whilst not neglecting v) *intercultural aspects* and vi) the *EU context*.

ZUSAMMENFASSUNG

Die *erste Zielstellung* ist, durch die phänomenologische Methode wohlbegründete Begriffe zu entwickeln, indem man elementare Phänomene der heutigen Welt mit einem Augenmerk auf die *Privatheit* und das *Digitale* durchdenkt, um zu beleuchten, *wer* wir sind in der Cyberwelt – also eine Phänomenologie des *digitalen Werseins*. Die *zweite Zielstellung* ist, durch die hermeneutische Methode eine Auseinandersetzung mit älterer sowie neuerer Literatur zur Privatheit einschließlich in der heute entstehenden Cyberwelt zu führen, deren wichtigste Ergebnisse Kritiken der lediglich *informationellen* Privatheit sowie des *autonomen Subjekts* gegenüber einer *objektiven, verdinglichten Welt* enthalten – im Gegensatz zu einem Selbst, das stets in gesellschaftlichen Machtspielen eingelassen ist. Phänomenologische Ergebnisse umfassen u. a. i) *Selbstidentität* durch ein *Interplay* mit der Welt, ii) *persönliche Privatheit* im Unterschied zur *Privatheit des Privateigentums*, iii) die *Cyberwelt* als künstliche, digitale Dimension, um schließlich zu diskutieren, iv) was *Freiheit* in der Cyberwelt bedeuten kann, ohne dabei v) *interkulturelle Aspekte* sowie vi) den *EU-Kontext* zu vernachlässigen.

[171] This is an abridged version; the full version is forthcoming in 2013.

2.1 INTRODUCTION

Rafael Capurro

The concept of privacy cannot be adequately determined without its counterpart, publicness. Privacy and publicness are not properties of things, data or persons, but rather ascriptions dependent upon the specific social and cultural context. These ascriptions relate to what a person or a self (it may also be several selves) divulges about him- or herself. A self, in turn, is not a worldless, isolated subject, but a human being who is and understands herself always already connected with others in a shared world. The possibility of hiding, of displaying or showing oneself off as who one is, no matter in what way and context and to what purpose, is in this sense, as far as we know, peculiar to human beings, but precisely not as the property of a subject, but rather as a form of the interplay of a human being's life as shared with others.

This, in turn, implies that the possibility of revealing and concealing who one is is always already concretely shaped within the rules of interplay of a concrete culture within a shared world. I understand by culture the totality of values, customs and principles on which a society is explicitly and implicitly based. Accordingly, the very meaning of private and public varies depending on the culture, which does not imply that these meanings and practices are equivocal or incommensurable, for they occur in a shared world-openness constituted by a network of referential interconnections of signification. This network of interrelated signification is today marked deeply by digital information technologies.

World-openness is not only always already concretely structured semantically and pragmatically in the sense of a culture, but also subjected to an historical process of forming and shaping over time. What constitutes a world can change as a consequence of diverse, unpredictable events. When a culture changes, and not merely the situation, values and customs within a culture, then the sense of the difference between private and public also changes. Jürgen Habermas has shown this in relation to the structural transformation of the public sphere,[172] but only in presenting, so to speak, largely one half of the story. A structural transformation of the public sphere (or rather: publicness as a mode of social being) implies also a structural transformation of the private sphere (privateness as a mode of social being), and both can be reflected upon. The latter is the task of information ethics when it is a matter of problematizing given values, customary life-practices and principles of action, that is, an ethos, in connection with digital technologies and the cyberworld to which they have today given rise.

If today we proceed from the fact that on the basis of these technologies and, in particular, the internet, a structural transformation of publicness is taking place, then this holds true equally for privacy. Information technologies do not hover in empty space but are embedded in the cultural life of societies. The distinction public/private in connection with the cyberworld is a socially and culturally dependent difference. Cultural dependency means that differences in the understanding of information technologies must be discussed if an encapsulation of societies and cultures is to be avoided, through which a potential ground for *reciprocal* trust would be surrendered. It is plain from what has been said that such a ground is always provisional. Trust is essentially also a mood that is counterposed to the moods of unsureness, fear, anxiety, and even Angst and dread. If Angst reveals the groundlessness of human freedom, trust signifies something like the experience of the formation of a tentative ground on which we can depend on each other, no matter in what fragile forms and within which limits. Hence trust does not signify, at least not primarily, putting oneself into the hands of another in line with the sentiment, 'Trust me, I'll look after you'. That is a particular form of (paternalistic) trust that is fostered, for instance, between parents and their children. In contrast to this (and there are many intermediate shades and variants of trust),

[172] Habermas 1962/1990.

reciprocal trust means that a self lets itself in for an interplay with other selves in certain situations and contexts, for which then customs, norms and values, including ethical and moral and legal usages and norms, are required to give this interplay a certain consistency and constancy, that is, some sort of ground. In this ongoing interplay, trust is engendered, won, put at risk, lost, etc. but never produced like a thing.

To foster trust in a globalized world and with respect to the artificial dimension of the cyberworld is certainly no easy task. The objective of the ethics strand within the present overall project consists in providing the foundations for a phenomenological explication of privacy and publicness in the context of the cyberworld enabled by digital information technologies. This will enable options for shaping life-worlds to be uncovered that are both shared and also culturally differentiated with regard to valued, customary living practices. Accordingly, everything will depend upon whether privacy and publicness and their respective socio-ontological foundations, no matter how provisionally, can be attuned and brought into play with each other so that differing, but nevertheless mutually permeable, casts of good living in the world can be outlined. From what has been said it is plain that in this ethical part of the project, the phenomenon of the self as well as that of a shared digitized world, the cyberworld, are given special weight and significance. The distinction between self and thing or, more precisely, between *who* and *what*, is the ethical difference from which the difference private/public can be thought. Therefore we take pains to spell out what whoness means.

The significance of a phenomenology of whoness as the starting-point for discussing the question concerning privacy and freedom in the internet

The difference between self and thing, or who and what, already points to the necessity of working out and presenting a phenomenology of whoness in a turn away from the modern 'matter-of-fact' subjectivity of a worldless subject vis-à-vis an objective world, an ontology which is tacitly presupposed as the framework for reflecting upon privacy, identity and freedom in the internet age. In contrast to this, the who is always already in the world and has an identity, whose phenomenological concept has to be explicitly unfolded whereas, strictly speaking, the worldless subject cannot have an identity, a point that will be made clear through engaging critically with selected authors. Identity is only possible where a who finds itself mirrored back from the world, and chooses, casts and takes on its self from this shining-back from the world. This is an essential hallmark of *freedom*, since the who fashions its self from the mirrored-back options including, above all, the world of others.

A provisional stocktaking of the discussion in information ethics on privacy and freedom in the internet age

The discussion in information ethics on the concept of privacy has changed and intensified over the past fifteen years due to the broad commercial and social use of the internet. This discussion sometimes assumes an ideological flavour when privacy in the internet age is declared to be obsolete or, conversely, defended in its traditional sense, frequently without having understood the unique, new, existential possibilities and even new, valuable, systematic, social formations that are emerging. Often cultural differences and specificities are left out of consideration in favour of considering human beings simply as apparently autonomous subjects in the Western sense. Analyses in information ethics show, for instance, that conceptions of privacy in Buddhist cultures are the complete opposite to those in Western cultures, but that nevertheless reasons can be given for why privacy in Buddhist cultures still can be regarded as worthy of protection in an ethical and legal sense. Such a discussion is still in its nascent stages, for instance, with regard to Latin American and African cultures.

To what extent and in what form can universalist approaches such as the Declaration of Principles made by the World Summit on the Information Society, or the Internet Rights &

Principles Coalition pay regard to the particularities and singularities of differing cultures, as well as to concrete 'good practices', when both global and local cultures of trust and privacy in the internet are to be engendered? Who are we when we are in the cyberworld? What does it mean to have a digital identity? And how can one's identity wander off into the cyberworld? In the debate in information ethics on privacy in the cyberworld, this question is understood mostly in the sense of '*What* are we when we are in the internet?'. It then concerns digital data on individual persons that are to be protected legally and ethically. Implicitly, however, this question includes also the question concerning *who* in the sense of the person to whom the data relate, revealing and concealing *who* this person is. When the question concerning who crops up in the discussion in information ethics, it does so usually in the guise of implicit, and therefore unclarified, preconception of what 'whoness' and 'personhood' mean.[173]

The debate over privacy thus presupposes and skips over the philosophical interpretation of what whoness means in the digital age. It begs the question. The question cannot be answered through a digital reduction that equates whoness simply with digital information about a person, or even declares personhood itself to be (ontologically) an informational data bundle, for such a reductionism leaves open the question concerning how 'person' is to be understood, what the specifically digital dimension is in a conceptually clarified sense, and what the interplay is among these phenomena. The philosophical-ethical foundations are either missing entirely – as in the current discussion on privacy and the internet, where the protection of privacy is simply presupposed as a 'value' without any phenomenological-conceptual clarification –, or the foundations are borrowed unquestioningly from subjectivist metaphysics, that is caught in its subject/object split, or else the digital itself as a mode of being, i. e. of how beings come to presence and shape up, is not laid out at all or only cursorily.

2.2 PHENOMENOLOGY OF WHONESS: IDENTITY, PRIVACY, TRUST AND FREEDOM

Michael Eldred[174]

In this chapter, the phenomenon of *whoness* will be illuminated in its various facets with respect to privacy, publicness and freedom. A phenomenology of whoness thus serves as a foundation for approaching *privacy*. The following chapter will then present a sketch of *digital ontology* as a basis paving the way to the succeeding chapter, which investigates whoness and privacy specifically in a *digitally* mediated world.

2.2.1 THE TRACE OF WHONESS STARTS WITH THE GREEKS

Humans beings share a world together. They are always already a *plurality*. Whoness is the phenomenon of a plurality of human beings who show themselves to each other in a shared world. A phenomenon is a showing, a disclosing, a revealing which, in its broadest sense, encompasses also the privative or negative modes of disclosing: concealing and revealing only distortedly. Because whoness is the phenomenon of human beings ('men' in older discourse) showing themselves *to each other*, it cannot be located in a single human being like a 'what', as in: 'What's that?' 'A stone.' There is also a reciprocity in human beings showing themselves *to each other*. This observation is key for approaching the phenomenon of whoness as distinct from that of whatness, which has a rich tradition in metaphysics starting with Plato and Aristotle. Whatness has been thought in this tradition as οὐσία, substance, essence, quidditas, etc. whereas whoness has tended to be subsumed under the metaphysical determinations of whatness. The distinction between what and who, quid and quis has not attracted the sharp focus of philosophical thinking, as evidenced by the

[173] Tavani 2008; Van den Hoven 2008.

[174] All sections of this chapter are the final authorial responsibility of Michael Eldred, apart from sections 2.2.9 and 2.2.10 by Rafael Capurro.

very absence of the apt words 'whoness' and 'quissity' in English. Thus, for example, what a human being is has been determined metaphysically as an animal with a soul and intellect. The trace of whoness, however, is not at all absent from the Western philosophical tradition but, instead of being treated in its own right as a mode of being, and thus as an ontological question, it has been relegated to the realm of ethics and politics, again starting with Plato and Aristotle. Whoness leaves its trace throughout Western thinking in phenomena and terms such as ἀνδρεία, φιλοτιμία (manliness/courage, love of esteem/honour/value, Plato), τιμή (esteem/honour/value, Aristotle), virtu (Machiavelli), vainglory (Hobbes), amour-propre (Rousseau), Anerkennung (Hegel) and so on, and only starts to come into its own with the originally German tradition of dialogical philosophy[175] and Heidegger, who focuses on casting human existence itself explicitly and ontologically under the heading of whoness (Wersein, Werheit).

Human beings showing themselves to each other can be regarded as their *showing off* to each other, their *self-display*, even to the point of hiding from each other exemplified in phenomena such as diffidence.[176] Human beings present themselves to each other in the open space of presence and, in doing so, show themselves off *as* who they are. Such showing-off may be simply 'as a man' or 'as a woman', and the showing-off to each other implies *acknowledging* each other's presence, even in the privative mode of ignoring each other's presence, say, when travelling in a crowded underground train. A nod or a wave or a salute or some other slight bodily gesture already suffices to acknowledge each other's presence in which they show themselves off *as* some who or other. So, from the very start, there is an *interchange* or *interplay*, be it ever so minimal, among human beings in showing themselves off to each other in the presence of a shared world. For the moment, the focus is restricted to presence, leaving aside the two temporal modes of absence.

2.2.2 SELFHOOD AS AN IDENTIFICATION WITH REFLECTIONS FROM THE WORLD

It is important for showing-off to have oneself acknowledged by others *as* who one shows oneself to be. One chooses, or neglects to choose, one's masks for self-display in adopting this or that behaviour, wearing certain clothes rather than others,[177] etc. in order to be seen *as* who one presents oneself. The interplay with each other is always a reciprocal *estimating* of each other's self-presentations. Willy-nilly one presents oneself as some who or other, thus making a certain *impression* on others. Who one *is* is always a matter of having adopted certain *masks of identity* reflected from the world as offers of who one could be in the world. Each human being is an *origin* of his or her own self-movement and has an *effect* on the surroundings, changing them this way or that, intentionally or unintentionally. Moving ably and skilfully in the shared world in some sense and some fashion or other is bound up with adopting the masks of identity through which one understands oneself and also presents oneself to the world. Being estimated in a positive sense in presenting oneself to others is the phenomenon of *esteem*. Such esteeming estimation of one's self-presentation depends also on presenting, or at least seeming to present, oneself as a *capable* who in some sense or other, which will be estimated variously in different circles and

175 Starting with Ludwig Feuerbach and on through authors such as Martin Buber, Eugen Rosenstock-Huessy, Ferdinand Ebner, Eberhard Grisebach, Karl Heim, Gabriel Marcel, Friedrich Gogarten, Helmut Plessner, Adolf Reinach, Dietrich von Hildebrand, Wilhelm Schapp, Alfred Schütz, Ludwig Binswanger, Hermann Levin Goldschmidt, Emmanuel Lévinas and Hans-Georg Gadamer. Cf. Theunissen 1977 for a comprehensive overview of most of these authors.

176 Cf. Eldred 2008/2011 Chaps. 2 and 3 for more detail of a phenomenology of whoness. Cf. also the critical appraisal of Arendt further on in the present chapter.

177 "It [men's dress] not only covers nakedness, gratifies vanity, and creates pleasure for the eye, but it serves to advertise the social, profession or intellectual standing of the wearer." Woolf 1938/2007.

situations. A brain surgeon presenting himself at a medical congress will make a big splash, whereas at a football game, his who-mask *as* a brain surgeon is of no import and makes no special impression. In the negative sense, estimation amounts to not having one's self-presentation appreciated, but rather depreciated.

The core mask of identity borne by a who is one's own proper name, around which other masks cluster. Above all, it is a matter of adopting masks of *ability* reflected by the world, thus developing one's own potential abilities to developed personal *powers* of whatever kind. Each who ends up in some vocation, profession, job, social role or other, thus becoming who she or he is in living that role, and this is the mask of identity that somewho (L. quisquam), for the most part, presents to the world *as who* he or she is, being estimated and esteemed by the others in the interplay. Since human beings are estimated and esteemed above all on the basis of their *personal powers and abilities* as who they are, and because the exercise of such powers also effects some change or other in the world, the interplay of mutual estimation is always also a *power play*, especially in the sense of mutually estimating each others who-standing. At first and for the most part, one wishes to have one's developed powers and abilities, whatever they may be, esteemed by the others in the power play. One may *fail* in doing so. In sharing the world, human beings are constantly estimating and assessing each other's performances in presenting themselves *as* somewho or other through their powers and abilities, i. e. their *merit* as that which deserves esteem. Those of a similar who-standing are therefore, for the most part, in a *competitive rivalry* with one another.

The introduction of individual powers and abilities that have been adopted as masks of identity forces a widening of focus from the temporal mode of presence because such powers refer both to who one has become and also to who one may become in future. The estimation of one's abilities by the others gives rise to one's *reputation* as who one is, and reputation refers to how one has presented oneself to the world in the past, which is never past, because one has inevitably always already established or ruined one's reputation as who in some circle or other. Conversely, who one will become depends crucially also on one's potential being estimated by those who are in a position (especially parents and teachers) to foster the development of that potential to powers and abilities that an individual *actually has* at its disposal. Futhermore there is the *futural* aspect of whoness in the *ambition* that someone has to become such-and-such, usually by honing his or her abilities of whatever kind. Such ambition is always also linked to *as* who one wants to be regarded in the world and is thus tied intimately to the power play of mutual estimation. Ambition is the striving to leave one's mark on the world, even to the point of establishing one's *fame* as someone about whom the 'world' speaks. Leaving one's mark on the world is a way of making an impression on the shared world, namely, a *lasting* impression, which again refers to the temporal dimension of the past or beenness.

Wanting to make any impression at all on the world, let alone, wanting to have an impact or to leave one's mark on the world, are all manifestations of the *will to power to be who*. To be somewho in the world amounts to having one's self-presentation to the world estimated, esteemed and reflected by the world, to *come to stand* in shared presence as a who with some standing. In the realm of politics, for example, a who may come to stand by being appointed or elected to a recognized political office, which thereby becomes a mask of identity for this particular individual who thus enjoys the *honour* of holding public office for as long as the specifically political power play accords the office in question to the individual in question. Such *standing presence*, however, is very fragile, not just in politics, but in the power play of togetherness in general, for it depends on the mirror game of mutal self-presentation in which having a stand as who depends on the reflections of estimation received back from the others.

2.2.3 VALUES, ETHOS, ETHICS

The question concerning values[178] has a close relationship with the phenomenon of esteem, which amounts to valuing someone *as* somewho. But values extend beyond whos to all sorts of things, including useful things (use-values), exchangeable things (exchange-values, money) and even intangible values such as local traditional customs, freedom of speech, freedom of religion, etc. etc. A value is what is valued, i. e. estimated highly, by a plurality of human beings living together in some way, whether on a small (community) or large (social) scale, contributing in some sense to living well in the context of everyday, customary life-practices. All societies cultivate usages through which they value and esteem each other in an interplay of mutual estimation, which gives a connection to the phenomenon of whoness that is foundational for the present study. Furthermore, things that are *good for living* have worth and value in all societies. The value of (commodity) goods is estimated through market exchange. Such valuation interplay is a reified (from *res* for 'thing') form of estimating and esteeming, as signalled already by the Greek τιμή which, apart from meaning the esteem or honour in which a person is held as somewho, signifies also the value or price of goods as somewhats. The valuing that goes on in social interplay is a component part of all historical peoples' ways of living and therefore *abstract* relative to the more *concrete* customs and traditions valued by particular peoples. As we shall see, this more abstract level of values and estimation is at the heart of liberal values (see below *2.2.5 The private individual, liberty, private property (Locke)*).

Since the usages within which human beings live together are historical in the sense of belonging to a particular time and a particular region, they vary, and therefore what is valued as being part of a customary way of life is also historically variable. Furthermore, any plurality of human beings living together will not be unanimous about what, in particular, is to be valued in customary life practices, so that there is always also tension, conflict and even struggle and war over the values according to which a plurality is to customarily live together. Even an absolutist regime, despite appeals even to sacred texts or traditions or divine empowerment, for instance, cannot dictate the values according to which a plurality of people is to live; there will always be dissent, whether covert or overt. Which values, in the sense of valued and esteemed customary practices, are upheld by a way of life is always a matter of the ongoing interplay among people in an historical time-space (cf. *2.5 Intercultural aspects of digitally mediated whoness, privacy and freedom*). Hence, like the striving to be esteemed as who, values themselves, especially the basic ones on which a shared way of living is founded, are exposed to an ongoing historical power play in which much depends upon disclosing what precisely is being valued and esteemed. Esteem, estimation, values, social power are always and essentially found together since they are socio-ontologically interlinked. This is invariably overlooked when values are simply posited to be such, or proclaimed to be 'fundamental', as if they had fallen from heaven or arose in a 'state of nature'.

Because values in the sense of valued and esteemed customary practices make up a way of life, taken together they form an ethos. *Ethics* pertains to how to live well within the ethos of an historical way of life shared by a people, i. e. within its complex of values in the sense of what is held dearly in the context of that way of life. Ethics has to be distinguished from *morality* and normativity, which are focused on the question of the actions an *individual ought* to do or refrain from doing, either generally or in a particular situation, hence bringing into play also matters of *conscience* and *compliance*.

[178] Cf. Eldred 2010.

2.2.4 THE QUESTION CONCERNING RIGHTS: PERSONAL PRIVACY, TRUST AND INTIMACY

Whenever the question concerning values crops up, the question concerning rights is never far behind, for what is estimated to be valuable for a way of life is held to be also indispensable for it and hence as making a claim to be protected, guaranteed, secured. Rights invariably pertain to individual human beings in their life movements and, by extension, to groups and communities of individuals. A *right* is a *claim* to a *guaranteed freedom of life-movement* in one sense or another (cf. *2.6 Ethical issues around the cyberworld and privacy in connection with basic EU values and principles*).

One kind of individual free life-movement is that of withdrawing into *privacy*, which is always a *privatio* in the sense of a withdrawal from (public) disclosure into concealment. Being able to withdraw or to reveal only those aspects of who one is and one's own life-world is valued in diverse cultural ways of living, albeit that the social interplay of such concealment and disclosure takes diverse phenomenal forms and is protected by diverse customs. Because each individual is somewho, this means showing oneself off in the shared world *as* who one is. This *as* signifies the masks with which each who identifies in pretending to be who he or she is. Such pretence is not to be contrasted with a 'genuine' who who would appear, as it were, naked, without mask, but rather, pretence itself is inevitable to be a who at all, and the question is only whether the identity adopted by a self is fitting or not. 'Masks' here cover all the ways in which somewho can present him- or herself to the world and to him- or herself; they are the identities adopted in a shining-back from the world, as explicated in previous sections. Self-showing in the world is hence a presentation that is also a matter of the self freely casting *as* who it shows itself off to the world. This may be choosing clothes to wear, or it may be writing a book or a letter to the editor of a newspaper, or adopting a certain vocation or profession, etc. etc. In each case a *persona* is presented to the world. Withdrawing from the shared world means leaving this persona aside in favour of more intimate and idiosyncratic masks of comportment presented only within the small circle of intimacy that was traditionally the family. The private person is still a who, but this private person shows itself only within a small circle of friends and family on a basis of familiarity and *trust* that such who-presentation does not become the common currency of mere gossip in the world.

Personal privacy is therefore never the privacy of an individual, encapsulated, autonomous subject, "being let alone" in splendid isolation or brooding introspection, but the hiddenness of a private life-world shared with certain others to whom one is close and from which most are excluded. The key to understanding personal privacy is the play of *disclosure and concealment of a personal world*. Others are only admitted to a personal world on a basis of trust and friendship. Within a circle of private intimacy, the individual whos present themselves *as* who they are, but this *as* deviates from the persona presented to the outer world. Such personal privacy is *valued* as one of the goods of living; it is a *privatio* to having to have one's self exposed to general public view. To gain one's own self requires not only adopting certain chosen possibilities of identification shone back from the world, but also withdrawing from common opinions about who one is or ought to be in order to decide freely which masks of identity are one's very own.

There are also *many* personal private lives; who I am comes about with each you I encounter, and each time anew. With you I show myself as ..., and with you I show myself as ...; and conversely for you: your masks of self-presentation change according to whom you are encountering, in a specific situation and at different times. Thus you, too, play a game of revealing and concealing who you are. The enjoyment of private life resides largely in the multiple games of who-presentation played within it. In public life, too, the who-presentations are multiple, depending upon situation; the

personae vary according to occasion, and differ from the who-presentations in the shelteredness of private life, where a who may risk other disclosures to an intimate. Who you and I are in an intimate sexual relationship, for instance, has its own special, unique flavour. Friends esteem each other by appreciating each other's company and messages.

Privacy also cannot be localized in a particular place, although the *home* has special importance as a sheltered place, sheltered above all from the gaze and hence idle talk and the abuse of private information by others. The private world can 'be' a conversation carried on with a friend in a pub or a restaurant or on a bus, each of which is a public-private place. The intermingling of privacy and publicness, which happens 'physically' all the time, will be treated further in *2.4.7 An appraisal of Nissenbaum's Privacy in Context*.

The phenomenon discussed so far is that of *personal privacy*, which has dominated discussions of privacy in connection with the internet. However, this discussion is truncated insofar as privacy extends to shared worlds that are not characterized by familiarity or intimacy, but are nevertheless germane to any phenomenology of privacy in today's world. In particular, the question concerning justice in relation to privacy should be postponed until the phenomenology of privacy has been widened to take in also private property and its manifold consequences. What is the privacy of private property?

2.2.5 THE PRIVATE INDIVIDUAL, LIBERTY, PRIVATE PROPERTY (LOCKE)

In this section featuring Locke as the father of liberalism, one could well imagine that we have arrived at the heart of a liberal worldview highly specific to the West. Indeed, Locke's famous formula of "Life, Liberty and Estate" as a fundamental, individualized right is at the core of liberalism. Taken as an inalienable, fundamental right of the individual, Locke's formula serves as a bulwark against all kinds of government interference, and that most pronouncedly so in Anglo-Saxon countries. Already in other parts of the West, such as Germany, this liberal value has not taken nearly so strong a root in the customary practices of living, even though a country such as Germany is still counted among the 'Western liberal democracies'. So liberalism itself has many, finely graduated hues in various countries. Western liberal values are also said to have been exported to the rest of the world, imposed upon other cultures (historical ways of living) by the West, or welcomed as influences voicing a critique or and promising liberation from customs and ways of governing felt already within those cultures to be oppressive and stifling.

Western liberal values of "Life, Liberty and Estate" have a meaning and make living sense in many different cultures, even when they are strongly diluted and relativized, or interpreted differently, by other valued customs and ideas within which an historical people lives. This is so because there is a deep, incontrovertible phenomenological grounding at least of individual life and liberty insofar as each individual human being is ineluctably and irrevocably a free source of its own life-movements of all kinds, even when it submits to a superior other, no matter what that other might be (a ruler, a state, a customary ethical order, a religion, etc. demanding submission). Rather than being regarded as 'inherent', 'natural' rights of individuals, life and liberty are *abstract values* arising from human being itself irrevocably individualized in origins of free self-movement. This does not have to do with any 'original' 'state of nature' but rather with the 'nature' of human being itself on an abstract level, where abstractness refers to the simplicity of few determinations.

Unlike life and liberty, private property cannot make such universal claims as a value of living, although each individual's and each individual family's goods and chattels, whatever they may be, and their enjoyment, are everywhere

prized and valued. Even the most paltry goods and chattels are private property, at least in the meagre sense of excluding others from their use, and such privacy of the use of things is valued even when it is not protected as a right. Article 17 of the Universal Declaration of Human Rights proclaims generally a right to property.

To deepen insight into the privateness of private property, the kinds of private property must be extended and the understanding thereof deepened in the sense of private property's being the basis for an entire economic way of life known as *capitalism*.

2.2.6 THE PRIVATE INDIVIDUAL AND PRIVATE PROPERTY AS A MODE OF REIFIED SOCIATION: THE GAINFUL GAME (CLASSICAL POLITICAL ECONOMY, MARX)

Although Locke proceeds from a heap of atomistically independent individuals with inalienable natural rights, in truth, the existence of the modern individual is itself the consequence of the establishment of a form of sociation through private property, whose ownership frees individuals from other kinds of social and political bonds, thus allowing them socio-ontologically to *be* individuals in the first place in a certain historical world that is still open today. To put it more sharply: the autonomous individual of modernity has always been an illusion, unbudgingly upheld to the present day in all 'bourgeois' discourses, resulting from wilful blindness to the socio-ontological condition of possibility of the free individual, namely, sociation through reified value. Locke's political philosophy, a grounding of liberalism of world-historical significance, ushers in also the moral-philosophical discussions of political economy in the eighteenth century and the emergence of the first proper social science, viz. economics. Hence Adam Smith becomes the father of economics, still revered today.

Karl Marx's various writings on the *Critique of Political Economy* clarify many of the antinomies in classical political economy, and works out that there are fundamentally *four* sorts of revenue, *four* revenue-sources and *four* social classes in a capitalist economy: *leased land* being the source of *ground-rent*, *invested capital* in an enterprise being the source of *profit* (of enterprise), *loaned money-capital* the source of *interest*, and *hired labour-power* of labourers the source of *wages*. Despite all the myriad changes that capitalism has gone through since the eighteenth century, so that today's capitalism is hardly recognizable in the mirror of older capitalist societies, the four fundamental categories of revenues and revenue-sources remain the same, although adopting many different deceptive guises in endless configurations and superpositions. This foursome of the "troika formula"[179] must be taken as giving the fundamental socio-ontological structure of capitalism, a very simple structure of forms of private property as income-source and income (to employ an alternative term to 'revenue') that can adopt infinitely many different configurations in the course of historical time and in different parts of the world.

In a capitalist economy, all the players are engaged in earning income by deploying their income-sources in the competitive play. The linchpin that holds together and mediates a capitalist economy is money(-capital), the crystalline, pure, reified form of *value* that can adopt also other forms, viz. commodity, wages, profit of enterprise, interest and ground-rent. The income type, profit of enterprise, can be capitalized as the price of an enterprise and ground-rent capitalized as the price of land. The labourer himself, however, can only hire out his labour power and cannot be capitalized as the price of a labourer, for that would violate the labourer's inalienable liberty. 'Labourer' itself is a misleading term because in this general context it comprises all those employed by a capitalist enterprise, including the managers and even the executives. Here is not the place to discuss details.[180]

[179] Eldred 1984/1910, § 7.
[180] Cf. Eldred 1984/2010.

Marx's great discovery and achievement, occluded by the historical course of Marxism, was to work out the essential socio-ontological structure of capitalism as an (augmentative) *movement of value through its various value-forms*, something that is not appreciated even today. Value is the medium of sociation (Vergesellschaftung) in capitalism. It is not a substance but a fleeting reflection that comes about on the various kinds of markets through the valuation interplay among buyers and sellers, lenders and borrowers, lessors and lessees, employers and employees. Because value is reified, however, it *seems* to have a substance. To move as capital, value has to strip off its monetary form and *risk* a movement through the circuit of capital in which it assumes other value-forms before returning as the principal advanced plus profit (which could turn out to be negative). Capitalism is an historical form of economic life that moves by virtue of an ongoing, constantly fluctuating, estimating interplay among people and things. The economic competition for income by deploying income-sources is the play of a capitalist economy itself which I therefore call the *gainful game*. However, nota bene: "In this broad sense of gainful game as an historical constellation *as* which the world shapes up, the winner can just as well be a loser."[181] Value thus assumes various thingly forms in the course of its movement, exercising its *social power* to transform itself.

Hence capitalism, or the gainful game, is a *reified* form of sociation differing from other historical worlds based on personal social power relations of direct subjugation. This elaborated socio-ontological structure implies already that it is very naïve and inadequate to speak simply of private property, especially when trying to throw light upon the privacy of private property, in particular in contradistinction to *personal* privacy, which is the dominant notion of privacy operative in current discussions of privacy and the internet. Private property in its fourfold income-source structure enables in the first place the gainful game of individual and joint players in that competitive game. Only because value itself, in its various value-form guises, has become *the* medium of sociation in the capitalist world, does such a thing as an *individual* exist at all historically.

2.2.7 TRUST AS THE GAINFUL GAME'S ELEMENT AND THE PRIVACY OF PRIVATE PROPERTY

The gainful game is played by players striving above all to earn income of the four basic kinds, or countless hybrids of these, by deploying their income-sources in the competitive economic interplay. The outcome of this striving is by no means certain; the movement of the gainful game is risky. The players meet each other on various kinds of markets, mutually estimating and evaluating each other with regard to what they have to offer, whether it be personal powers and abilities (labour power) or a thingly productive power, be it produced goods, land, means of production or loan-capital, each of which has a price that fluctuates constantly according to the way the market-valuation interplay plays out. The players come to exchange agreements within the framework of *contract*, which is the appropriate form of intercourse for the economic gainful game. In addition, the players have to estimate each other's *credibility, trustworthiness* and especially *credit-worthiness*, since the gainful game can only be played if the players *keep their word* and fulfil their contracts properly. "That men performe their Covenants made"[182] is at the heart of Hobbes' conception of justice which is thus one of *commutative* justice (cf. *2.2.8 Justice and state protection of privacy*). Since the markets are subject to constant fluctuations in valuation, the players' credit-worthiness is also all-important to ensure that payments are made even if economic circumstances worsen. Credit-worthiness is an *estimation* of *who* the potential contractual partner *is*, i. e. his or her *reputation* based on others' opinions of the person's *reliability* and an assessment of how the person lives, i. e. which existential options he or she has realized, especially with regard to assets

[181] Eldred 2000/2010.
[182] Hobbes 1651/1997, p. 71.

or debts accumulated. Clearing up doubts about credit-worthiness removes the healthy mistrust that is part of playing the gainful game, paving the way for a transaction. When credibility and *trust* among the players evaporate, or when the momentary prospects for making a gain worsen, valuations on the market deflate or even collapse, and the gainful game slows or seizes up.

What can be said specifically of the *privacy* of private property in contrast to personal privacy? First of all there are the things that an individual (or individual's family) owns, enjoying them in personal life. Income acquired in the gainful game is spent on goods that are privately used, excluding others from their use and enjoyment. Privacy here means not so much *concealment* but *exclusion* of use by others. This applies also to privately owned land and to personal bank accounts; the individual decides who has access to his or her home and decides freely over how to exercise the power of acquired money when spending it. Such free disposal of income is an essential feature of liberal freedom that ties liberty to private property. Since reified value is the medium of sociation in a capitalist economy, in all its reifications, either as money or as saleable property of whatever kind, it is a *social power* to acquire through exchange which is fundamental to such a money-mediated way of life. Likewise, the striving for income depends crucially upon the estimated and validated value of what is offered on the market for valuation, including human labour power (abilities of all kinds), consumption goods, investment goods, land for lease, money-capital for loan. Hence all the various incomes and income-sources are themselves pieces in the *power play* to earn and spend income, thus exercising money's power to effect a change, i. e. an ex-change. The value power play is always a power play of estimation played out on diverse markets, and has diverse phenomenal forms. Accordingly, the privacy of the various kinds of property has very different phenomenal forms, e. g. the privacy of a piece of land looks very different from the privacy of a bank account or the privacy of an enterprise's premises or facilities, but all are characterized by a privation of access and disposal.

Privation of access, use and disposal is the hallmark of the *privacy of private property* rather than the concealment of who one is in one's personal life-world, which is the hallmark of personal privacy. Hence the privacy of private property can go hand in hand with its public display, the very opposite of concealment. Such public display lives from the tension that others have no access to the private property displayed in a game to enhance one's own who-standing. Look but don't touch. Here it is more than plain that being *a* who is itself a power play of presenting oneself in public in order to have an *impact* of some sort (i. e. to make a difference), to be esteemed in one way or another, perhaps in a game for validating one's own self-importance. The *public* display of *private* property for the sake of who-standing is contradictory in the sense of relying on two different, contradictory kinds of privation, perhaps to incite envy. The drive to *be a* who means the striving to display oneself for the sake of being esteemed and validated in some way. Personal privacy often amounts to withdrawing temporarily from such who-display in favour of enjoying a private world with family and friends.

2.2.8 JUSTICE AND STATE PROTECTION OF PRIVACY

The protection of personal privacy is an aspect of the protection of an individual's private *life*. Incursions by others into a person's private life may amount to revealing publicly details about that private life-*world*. Personal privacy must be thought of not as the privacy of an individual subject encapsulated within itself, but as the non-disclosure of a personal, individual life-world. Other aspects of the protection of an individual's private life include the protection of an individual's public persona, i. e. of the mask *as who* this individual presents him- or herself in public, thus revealing and showing off who he or she is. An important aspect of this public persona, in turn, is an individual's *reputation*,

which is *who* this individual is taken and *estimated* to be by the others, which is not simply a matter of who the individual presents himself to be in the present, but extends especially to the temporal dimension of the *memory* of how the individual's persona is publicly assessed (cf. *2.4.7 An appraisal of Nissenbaum's Privacy in Context*). Damage to reputation is at the heart of an injury to an individual's life, even though it is not a physical injury. There is a link between injuries to a person's reputation through libel and slander, on the one hand, and, on the other, prying into the private details of an individual's life-world in order then to publicly disclose, with malicious intent, reputationally damaging facts about the individual concerned. There is also a link between invasions of personal privacy and monetary gain when media publish private details in gossip-mongering fashion. The converse of protection against such invasions of personal privacy is the right of *freedom of speech* which is an essential feature of individual liberty with respect to both what can be said and revealed about the members of civil society and what can be said and revealed about the government and the state. Freedom of expression is an aspect of the freedom to show oneself *as who* one is, because the opinions, writings, art works, etc. which an individual places in the public realm are all who-masks with which that individual *identifies* (cf. *2.2.2 Selfhood as an identification with reflections from the world*).

What about the collection of facts about an individual's life that are in some sense already public, such as an individual's personal spending behaviour? Such data are collected automatically when an individual uses a credit or debit card to pay for consumer purchases which can be used to construct a profile of that individual's consumer preferences which, when combined with masses of similar profiles of other consumers, will give a profile of spending behaviour in a given region or a given market segment, etc. that, in turn, can be used to design advertising campaigns. Individual consumer profiles can be used to individually target an individual with specific advertising. Here there is no malicious intent to damage anyone's reputation, but rather the aim of making a monetary gain out of it. Such profiling has only become feasible with the advent of digital technologies. Hence treatment thereof as an issue of infringement of personal privacy will be deferred to later (cf. *2.4.2 Digital privacy: personal freedom to reveal and conceal*).

The other major aspect of the protection of personal privacy and private property concerns not the interplay within civil society, but the incursions of the state itself into privacy in the name of a higher good, viz., the well-being of the state and society as a whole. Such incursions are made for the sake of both commutative and (re)distributive justice. In the former case, privacy is invaded to fight crime, an important aspect of the protection of both private property, and individual life and liberty. Both the liberal and the welfare aspects of the state motivate it to curtail personal privacy and also private property for the sake of *raising taxes*. In particular, the state itself invades the private life-worlds of its tax-payers, and keeps tabs on their activities, to ensure the collection of taxation.

The *constitution* of a state is supposed to afford some protection against the government's invasions of privacy and incursions into private property, thus ameliorating also the arbitrariness of government taxation policy and its enforcement.

The gainful game is played today also beyond the boundaries of the modern nation state, in a globalized economy and indeed, the striving for gain was *the* major motor for globalization since the 15th century. Since national sovereignty is limited, other supranational political powers need to be instituted in order, in the first place, to provide internationally valid rules of play which amount to the international protection of life, liberty and private property and legal rules for the intercourse with private property that conform with rights to life and liberty (e. g. child labour) and promote the movement of the gainful game (e. g. bilateral and multilateral trade agreements). The Universal

Declaration of Human Rights proclaimed by the United Nations is perhaps the most general expression of an international will to uphold life, liberty (Article 3) and property (Article 17).

2.2.9 KANT'S FREE AUTONOMOUS SUBJECT AND *PRIVATIO* IN THE USE OF REASON

Rafael Capurro

Who are we humans? The core message of Kant's thinking on this question is that we are not just something or a "what" belonging to the sensory world that is governed by the (Newtonian) laws of physics but that we have a second nature beyond the "phenomenal" one that he calls "noumenal".[183] Noumenal beings, of which, according to Kant, there might be others apart from ourselves, humans, are free and autonomous. Kant's interpretation of human freedom as a "causality of freedom" is metaphysical, in contrast to a phenomenological perspective as addressed above in 2.2.5. Humans as noumenal beings are persons having "dignity" and not a "price".[184] As free and autonomous beings humans are subject to the moral law that compels them categorically to act according to universalizable maxims. Although the moral law makes evident the social nature of humans, its call does not originate from the encounter with another person but comes from within and beyond the subject due to its dual inner nature as encapsulated subject divorced from the world. The "true self" commands us to respect humanity in our being as persons.[185] Kantian thinking is dual. We are autonomous and heteronomous beings at the same time, but while our heteronomy with regard to natural laws is unavoidable, we are free to follow or refuse the moral call. There is a gap between our will and the moral law that is specific to the human being as "noumenal" or "intelligible", this not being the case with other "intelligible beings".[186] This Kantian dualism of the human self corresponds to the dualism between the sensory and the supersensuous or "noumenal" world, a view that Kant inherits from both Greek metaphysics and Christianity.

This conception of the free autonomous subject is contrasted by Kant with the constraints imposed on human reason by any kind of official duty that restricts the subject from using it freely and universally. In contrast to today's common use of the words 'public' and 'private' according to which an official duty is regarded as 'public', Kant stresses in 'An Answer to the Question: What is Enlightenment?' that the public use of reason as an office-holder is, in fact, 'private' ("Privatgebrauch") since it is not fully free and autonomous. This contrasts to the case where an individual – and Kant mentions explicitly the scholar ("Gelehrter") – employs its reason free of such constraints ("öffentlicher Gebrauch"), addressing "the whole public of the world of readers".[187] The ideal of the free autonomous subject using its reason without external constraints of office is thus something crucial for Kant and other thinkers of the Enlightenment, since it enables the subject to communicate his thoughts – Kant uses the masculine – without being subjected to censorship. It is Kant's intention to protect the free autonomous subject from official constraints by opening him to a potentially universal public through the use of printing technology ("die Schriften") as a medium. Kant's plea for protecting the "public use" of reason is, in today's terminology, a plea for freedom of speech of a free, autonomous subject.

It is important to note that for Kant this individual thinking and acting does not take place in isolation and is inseparable from the freedom to communicate using various media, particularly printing technology. For Kant, orality is a medium for the "private use" of reason, as in the case of religious, political

183 Kant 1977, A 65 p. 550.
184 Kant 1974, B 78 p. 68.
185 Kant 1974, BA 118 p. 95.
186 Kant 1974, BA 40 p. 43.
187 Kant 1975, A 485 p. 55.

or military leaders. It addresses a group of persons that is always limited or "domestic" ("häuslich").[188] Kant reverses, once again, not only today's common linguistic usage but, more importantly, the ethical values related to the concepts of "public" and "private". The public use of reason, which amounts to the individual's freedom of speech or expression in today's usage, is that specific to a free, autonomous individual scholar addressing the whole world of readers ("Leserwelt") which is at the same time the "society of world citizens" "(Weltbürgergesellschaft").[189] The scholar offers his thoughts "freely and publicly" "for critical examination" ("frei und öffentlich der Welt zur Prüfung darlegen").[190] This has a higher ethical value than the so-called 'public' or official use of reason as office-holders which for Kant is 'private' in the sense that it is a privation of its autonomous and free use. Hence, Kant's notion of privacy is opposite to the determination of personal privacy in the present study as a concealment of *who* one is, in the sense that a public office holder is *obliged* to subject the free use of his or her reason to an alien raison, which may be raison d'état or that of an association, a political party, an institution, a company, etc. *The right to personal privacy is inverted into an obligation to personal privacy*. This notion of an obligatory or forced privacy in showing off *who* one *is* through expressing what one thinks still has relevance today, sometimes in subtle ways. A public servant, for instance, may be prohibited from giving interviews to the media, which is an enforced privacy, but a politician also does not freely express what he thinks and in this sense restricts the free use of his reason, thus concealing *who* he 'truly' is, for political, tactical reasons relating to what he wants his electorate to hear. Something similar holds true mutatis mutandis for diplomats, heads of companies or organizations such as universities, etc. They are not free to choose the masks of who-presentation that truly fit.

Kant's insistence on this freedom of expression with regard to scholars is, in fact, arguably a pusillanimous compromise with political, religious and military powers. If scholarly freedom of expression, at least, is allowed, then, Kant gingerly suggests, there might be some hope that things might change for the better, since freedom of scholarly thought might induce "little by little" ("nach und nach") the general public to act more freely and live more in accordance with human dignity, humans being more than "mere machines".[191] This is what Kant calls the "true reform of the way of thinking" ("wahre Reform der Denkungsart").[192]

2.2.10 PRIVACY AS PROTECTION OF INDIVIDUAL AUTONOMY – ON RÖSSLER'S *THE VALUE OF PRIVACY*

Rafael Capurro

"The question of whom I live with is a private affair, and so is what I think about my colleagues at work." This is the first sentence of Beate Rössler's *The Value of Privacy*.[193] The book ends with a story, *The Private Life*, by Henry James (1843–1916), "about the possible dissociation of the private and the public self, the private and the public person."[194] These two quotes provide a hint as to what is at stake for Rössler when discussing "the value of privacy", namely, the protection of the self or, more precisely, the protection of individual autonomy, which includes "the protection *of* relations and *within* relations, protection *with* others and protection *from* others. Each of the three dimensions therefore also includes the protection of the solitary subject from all others."[195] This protection concerns the three dimensions of privacy that she identifies and analyzes in her book, namely decisional,

188 Kant 1975, A 488 p. 57.
189 Kant 1975, A 486 p. 56.
190 Kant 1975, A 292 p. 60.
191 Kant 1975, A. 494 p. 61.
192 Kant 1975, A 485 p. 55.
193 Rössler 2005, p. 1.
194 Rössler 2005, p. 188.
195 Rössler 2005, p 192.

informational and local privacy. Although acknowledging that one's personal life always includes relations with others, Rössler's concept of privacy focuses ultimately on the solitary autonomous subject. In the introduction she points to her use of the term 'private' as referring to "modes of action and conduct", "a certain knowledge" and "spaces", the third type being the view of privacy highlighted by Hannah Arendt on whom she later comments critically (cf. the following section). Issues of access and control – which she traces back to Warren and Brandeis' 'right to be left alone' as well as to Ruth Gavison and Alan F. Westin – form the core of Rössler's view of privacy. She writes, "Something counts as private if one can oneself control the access to this 'something'",[196] thus passing up the opportunity to distinguish between something and somewho. She broadens the issue of privacy beyond the classical notion based on spaces that I can control by discussing the value of privacy within the framework of liberal democracy that aims at protecting "individual freedom and the autonomy of persons in the face of inadmissible interference or regulations on the part of the state."[197]

According to Rössler, egalitarian liberalism is based on four principles, namely liberty, equality, neutrality of the state and democracy. Nonetheless, she is aware of the cultural differences in the normative conception of privacy and autonomy not only between Western and non-Western, but also within Western liberal societies such as in the case of the U.S. and Germany which she scrutinizes. She maintains that the U.S. conception of privacy is based on the view that the state must keep a distance from the decisions and actions of the individual, while in Germany – she points particularly to the *Großer Lauschangriff* ('the great bugging operation') – it is less about state *intrusions* than about *inspections* of one's life.[198] She underscores that in both cases the ideal of a life "of one's own", understood as an autonomous and authentic life, depends upon privacy. A core issue in Rössler's view on privacy concerns the notion of freedom as individual autonomy, a concept that she traces back to Locke, Kant and Mill as well as to Rawls and Habermas. She analyzes the critique of the liberal tradition raised by feminist theories concerning the concept of privacy as being gender-biased.

Freedom, she argues, does not centre on what I can do or not do, or what I have the opportunity to do or not to do, since such contingencies are beyond human influence. The lack of ability to do something does not equate to a lack of freedom. The notions of freedom and autonomy are taken from the classic liberal tradition of Kant and Mill. She does not reduce the concept of autonomy to the Kantian sense of *moral* autonomy but enlarges it to that of "*personal* autonomy in the sense of general personal self-determination concerning how I want to lead my life."[199] Privacy has to do with the protection of this evaluative view of oneself, i. e. with our desires, goals and values and "*her own good reasons*" "to understand herself as the author of an action", as she remarks, following Gerald Dworkin and Richard Lindley.[200] She regards this critical attitude toward oneself as the core of the idea of authenticity as developed by Charles Taylor. She stresses that the question of giving oneself priorities with regard to projects and goals is not an easy task and that the range of options is determined by the cultural background as well as by the social context.[201] To be autonomous does not imply being exempt from such predeterminations, but being able to reflect on them. She rejects theories whose concept of privacy focuses solely on the protection of relations or on that of the person herself. The reason is "because neither of them is able to do justice to *all* the key aspects of privacy [...] Special rights to privacy do not necessarily need to be based on the protection of "individual *freedom* or the

196 Rössler 2005, p. 8
197 Rössler 2005, p. 10.
198 Rössler 2005, p. 14.
199 Rössler 2005, p. 51.
200 Rössler 2005, p. 54.
201 Rössler 2005, p. 64.

inviolability of persons."[202] This is why she rejects the view of privacy as being primarily concerned with the protection of freedom and not of autonomy.

She summarizes her key insight as follows, "The thesis I am concerned with is that the true realization of freedom, that is a life led autonomously, is only possible in conditions where privacy is protected."[203] Privacy-protecting autonomy is the basis of freedom, not the other way round. "Why do we like having 'a room of our own?'? Why do we want it to be in our hands what our colleagues know about our private life?" she asks. And her answer is, "Because all of this [...] would encroach upon our autonomy. To be able to ask oneself authentically who one is and how one would like to live, it is clearly necessary to have possibilities of withdrawing from the gaze of other people. To be able to conceive, develop and pursue goals, it is necessary to have dimensions in one's life that are free from the objections or control of other people."[204] Rössler does not see that the private, autonomous individual is always already in the world and that this world as a social world is sociated (vergesellschaftet) precisely by *reified social interplay* that provides the socio-ontological conditions of possibility of the historical modern individual as an individual (cf. *2.2.6 The private individual and private property as a mode of reified sociation: the gainful game (classical political economy, Marx)*). Privacy as autonomy-protection means, for Rössler, being able to control the access "of others to me, to my person, to my (reflections on) decisions, and to information upon me."[205] This lays the foundation for the three dimensions of privacy, namely decisional, informational and local. Following, but also criticizing, ideas by Mill and Rorty, she deals with decisional privacy as being at the core of a self-determined life. Both authors separate the public sphere as the realm of liberal justice from the private domain where the individual's freedom and self-casting can unfold. Rössler criticizes not only the underlying assumption of a dichotomy between two separate spheres but rejects also the identification of privacy and freedom in the crude sense that to be free is ultimately to be private. She writes, "Yet what would, in certain circumstances, be violated is my (decisional) privacy, the opportunity for me to behave or live *unhampered* as I wish in social space. In such a conflict, one would appeal not to principles of liberty but of privacy."[206]

The autonomous private self in its solitude, who is at the heart of Rössler's "value of privacy", is only ever the converse side of the heteronomous, public self who is exposed to the finitude and vulnerability of human existence in the world. To *be* somewho requires showing off who one is in the world. A who is also endowed with the capacity, i. e. the power, as a self of sharing a common world-openness to provide different responses to the inexhaustible call(s) of being. This is the utmost task of the human evaluator, her ownmost, singular and inalienable personal task, which is proper (ἴδιος) or 'private' to her as a self but that she can forfeit, say, by either identifying or becoming identified with her (digital) data as a digital object of exchange in the cyberworld (cf. *2.3.5 The parallel cyberworld that fits like a glove* and *2.4.5 Freedom in the cyberworld*). This is *one* way in which the self can lose its self to everyday averageness today.

2.2.11 ARENDT ON WHONESS IN THE WORLD[207]

Arendt's discovery of the plurality of whos in *The Human Condition*

Perhaps the most exciting chapter in Hannah Arendt's major work, *The Human Condition*,[208] is the pivotal Chapter V

202 Rössler 2005, pp. 70f.
203 Rössler 2005, p. 72.
204 Rössler 2005, p. 73.
205 Rössler 2005, p. 73.
206 Rössler 2005, p. 83.
207 This entire section is the final authorial responsibility of Michael Eldred.
208 Arendt 1958/1998.

on Action, completing the triad of the work's central trichotomy between labour, work and action. If labour for Arendt is the movement of the natural life-process of human being itself, based on biological need, and work is the movement of production that brings forth the works constituting an enduring, stable, material world, the realm of action is the movement of action and speech constituting what Arendt regards as the political realm proper. The chapter starts with an obvious, indeed seemingly trivial, observation, namely, that human beings exist in a "plurality",[209] thus taking up again an insight enunciated already in the first chapter, where Arendt pronounces plurality to be "the condition of human action" (1:9). This observation already offers the germ of the possibility of breaking with the venerable tradition of Western metaphysics of determining the human essence without recourse to the plurality of humankind as a determination that fundamentally affects any attempt to think human being itself.

In the section on Action, Arendt makes use of the insight into plurality to introduce the problematic of how human beings "disclose" themselves "to each other" (24:176) as "who" (24:178) in "speech and action" (Gk: λέξις, πρᾶξις cf. 4:25), human plurality itself being "the basic condition of both action and speech" (24:175). She sees clearly that the question regarding "*who* somebody is" (25:181) has to be clearly distinguished from that concerning "*what* he is" (25:181), where this what is explicated as "his qualities, gifts, talents, and shortcomings" (24:179) that he "shares with others like him" (25:181). The shift of focus to what, that is determined in the third person singular, has "the result that his specific uniqueness escapes us" (25:181). By contrast, who someone is, is disclosed to others through words and deeds, especially works and deeds of love, that reveal this who's uniqueness, which is impossible "without a name" (24:180). Bearing a unique, proper name is hence a hallmark of whoness, but Arendt does not say as much explicitly, although this lies deep in the Judaeo-Christian tradition.[210] Nor does she use the term 'whoness' or 'quissity' to mark this dimension of social interaction among human beings off from the traditional category of 'whatness' or 'quiddity'. "Who" for Arendt is in any case explicitly a category or dimension of disclosure, of revelation, and that within the shared public realm in which name-bearing "men" show to each other *who* they are through word and deed.

There is, however, no ontological follow-through in Arendt's presentation of the phenomenon of whoness (and not only of whoness). What she offers is a philosophical anthropology interwoven with historical observations from Western history, especially from Greek and Roman antiquity.

Nonetheless, Arendt's many novel and stimulating insights into the interplay that is human action deserve attention with a view to bringing them to their proper, elaborated socio-ontological concepts. To start with it must be noted that her use of the term 'action' (and 'interaction') is not a happy one because its difference from concepts of action and interaction, say, in Newtonian mechanics remains unclarified, and indeed, later on, gets thoroughly confused with them. A concept of interplay is entirely lacking and is at best only implicitly present, folded into the texture of her script, for instance, when she writes, "action, though it may proceed from nowhere, so to speak, acts into a medium where every reaction becomes a chain reaction" (26:190).

It is the character of the movement of human beings' togetherness as interplay, whose explicit ontological structure I have presented in detail elsewhere,[211] that lends "human affairs" the "frailty" (26:188ff) that Arendt attributes to them. The "web of relationships" (25:181ff) among whos, which Arendt regards merely as a "metaphor" (25:183) and

209 Arendt 1958/1998, Section 24 p. 175; hereafter cited in the form 24:175.

210 Already in Genesis (Gen. 2:7) it is said that Yahve created man (âdam; adâma=earth), thus making a normal word into a proper name in Gen. 4:25, und 5:3 (cf. the commentary to the Bible de Jérusalem, translated into French by L'Ecole biblique de Jérusalem, Paris 1961).

211 Cf. Eldred 2008/2011 and also Fink 2010.

not as a fully fledged concept, is likewise, ontologically speaking, the interplay in which human beings willy-nilly entangle themselves with one another already by virtue of sharing a world with one another. Arendt herself has the germ of a more adequate concept with "to be among men" (inter homines esse)" (1:7).

The question concerning whoness as the key question of social ontology

The question concerning whoness is the key question of human togetherness in the world. Although Arendt refers to Augustine as the source for this question in the history of philosophy, it is Heidegger who puts the question on the philosophical agenda as an existential-ontological question. Heidegger's Marburg lectures on *Fundamental Problems of Phenomenology* in Summer Semester 1927[212] question in depth the traditional determinations of human being as some kind of being-at-hand (Vorhandenheit), such as res cogitans or a moral subject, and open up an alternative casting of human being as Dasein that allows a radically different ontological understanding of the selfhood of the self by marking off what from who:

> The being that we are ourselves, Dasein [human existence, ME], cannot be *questioned* at all as such with the question, *what* is that? We only gain access to this being when we ask: *who* is it? Dasein is not constituted by whatness, but by whoness. The answer does not specify a thing, but an I, you, we. But, on the other hand, we ask nevertheless: *what* is this *who* and and this whoness of Dasein – what is who in distinction to the above-mentioned what in the narrow sense of the thingness of what is present-at-hand/occurrent. Doubtless we ask thus. But in doing so it is merely declared that this what with which we ask also for the essence of the who obviously cannot coincide with the what in the sense of whatness.[213]

This long quote rubs the question concerning whoness under our noses, so to speak. It cannot be left in any sort of implicitness if the core of existential ontology is to be worthy of the name. Here, drawing on my other work, only a few brief indications will be given of how whoness as the mode of human beings sharing a world with one another can be laid out. Arendt mentions, for example, that making an appearance in the public realm, i. e. action, "without a name, a 'who' attached to it is meaningless" (24:180). A who has an identity, and the core of this identity is the who's proper name. A singular human existence must be identified with something that it is not, namely, in the first place, with a proper name, in order to *be* a who at all. Identity as who therefore presupposes difference and, more than that, an identity of identity and difference, since identity itself includes difference within itself. Who someone *is* as him*self* is only possible as an identity with something *other*. If the public sphere is a realm of appearance in which all whos are play-acting in an interplay with one another, the first mask they bear is their proper names that identify who each *is* – including for each who itself. Each who is a dramatis persona, i. e. a person bearing a mask in a drama, i. e. an action, played out with other actors, and this is not a metaphor, but, on the contrary, the ontological fundament on which such a thing as play-acting on a theatre stage is possible at all.

Arendt restricts the human power to begin "something new on our own initiative" to acting: "To act, in its most general sense, means to take an initiative, to begin, (as the Greek word *archein*, 'to begin', 'to lead', and eventually 'to rule', indicates), to set something into motion (which is the original meaning of the Latin agere)," thereby bringing Greek ἀρχή into play, a concept that bears a heavy weight in Greek productivist metaphysics. "To set something into motion" in metaphysics means paradigmatically to be the starting-point (ἀρχή) for a *productive* activity as the power to bring about a change/movement of something ultimately

212 Heidegger GA24 1975.
213 Heidegger GA24 1975, p. 169.

into a finished product. From this ontology of productive movement/change, all philosophical understanding of movement is tacitly dominated, including Arendt's, even when she transplants the human power to be a beginning from productive activity to acting in the political sphere merely by omitting the end-product of productive movement, hence basically following Aristotle. 'Being a beginning', of course, cannot be limited to 'being born', i. e. to the natality that Arendt underscores, but means instead to power to cast oneself as a self into the temporal dimension of the future – at any time during one's existence.

Because she does not pay attention to the ontological structure of movement, Arendt also does not draw the necessary import from her insistence on the main thesis that action is always action among a *plurality* of "men", each of whom is a beginning, an ἀρχή.[214] If this is so, then the interactions among such men are the interplay among a plurality of ἀρχαί where the term 'interplay' is warranted to mark it off from the ontology of productive movement, which is an acting upon a physical thing (or a human regarded as a physical thing). Where a plurality of 'beginnings' are 'at play' with one another in action, what happens has the character of "inherent unpredictability", a character that Arendt sees only deriving from i) "the inability to foretell all the logical consequences of a particular act" (26:191) and ii) the inconclusiveness "of the story which, as the result of action, begins and establishes itself as soon as the fleeting moment of the deed is past", but can reveal "its full meaning [...] only when it has ended" (26:192).

Power, in Arendt's use of the word, "is what keeps the public realm, the potential space of appearance between acting and speaking men, in existence" (28:200). This can be translated by saying that power is the potential for playing the phallic who-game of standing presence among men and hence, in this translated sense is a "potentiality in being together" (28:201). Power in Arendt's sense is thus the potentiality keeping open the space for the who-game of standing presence. This *potential* is *actually* played out within this who-space as the *energy* (ἐνέργεια, at-workness) of mutual who-estimation and who-stand-contestation. Such potential is present above all in cities that provide a place for men to show themselves off to each other as who they are in a contest of mutual estimation whose ongoing outcomes remain incalculable. The "striving toward omnipotence" or "hubris" (28:202) can be interpreted as the striving for the highest stand as who, a futile striving insofar as an omnipotence would annihilate the potential for contestation among whos, as if other men were, or could ever be, entirely without power in the sense of lacking altogether the potency to make any change whatsoever in the world. Only dead men are impotent in this sense, and not even they are impotent insofar as their status, name and perhaps even fame as somewho *moves* those who are alive.

The untenability of the distinction between labour, work and action

After having clarified what is to be understood by action, I turn to Arendt's postulation of "three fundamental human activities" (1:7) corresponding to three different determinations of human being itself, namely, *animal laborans*, *homo faber* and *homo publicus* (whereby Arendt does not employ this last term). She has an historical paradigm in view in drawing these distinctions, namely, the Greek polis. The sphere for the first kind of activity is that of private, hidden existence concerned with biological needs and functions of the body, including especially birth and death, whose needs-fulfilment was achieved by the *labour* of slaves and women in the household. The second kind of activity is that of craftsmen's *work* making more durable things such as tables that are not immediately consumed in the satisfaction of need and therefore contribute to building a stable, durable world of things in which men live, i. e. a world's produced infrastructure. The third kind of activity, as we have seen more clearly through the explication above, is

[214] To be a beginning and thus free is a thought to be found throughout the metaphysical tradition, for instance with Kant (see above section) or Adam Smith: "...in the great chess-board of human society, every single piece has a principle of motion of its own..." Smith 1759/2000, Part VI, Section II Chapter II, penultimate paragraph p. 343.

that of *acting* as a who in a power play of mutual estimation, through which human existence comes to stand and shine in the shared world of the public realm.

Three different kinds of activity corresponding to three distinct, tacitly ontological, determinations of human being itself are already problematic, revealing a mixing of the ontic-factual with the ontological. The first determination of human being itself as *animal laborans* is already shaky because it reduces human being to needy animal being. Thus, on that level, the labour of a man making bread can be compared with the labour of a bee making honey as a biological necessity of life *sans phrase*. "To labor meant to be enslaved by necessity..." (11:83). Human existence is then conceived as the striving to fulfil needs which, as biological, are dictated by the life-process itself of birth through to death and its reproductive repetitition. But the way human beings live with one another is never simply a matter of fulfilling biological needs. Rather, biological need-fulfilment is sublated and embedded within the practices of everyday life that are always historical usages which themselves determine, in turn, what is needed. Naked biology in itself never defines need.[215] Furthermore, because needs are determined by the usages of sharing a world together, they are not limited to human 'species-being'. Hence, when Arendt argues in such a way, e. g. when she follows the well-worn ruts of theories of under-consumption and over-production in capitalism and argues that the "progress of accumulation of wealth" is subject to "the limitation imposed by the capacity to consume" (16:124), she is asserting a finiteness of human need. But needs are limitless because they grow out of the usages within which human beings share the world, doing things for each other. The possibilities of life-enhancing usages, however, are limitless and constantly changing through historical time.

Arendt laments that in the modern world, the activity of labour has been totalized to all of society. It has come out of hiding in the private sphere of the household and become the underlying category for society at large that is now become income-earning, consumerist society and conceived as an enormous household to be administered by "gigantic bureaucratic machines" (11:93). The realm of politics, she says, now becomes household management, and all human activities are evaluated according to whether they are productive or unproductive (cf. 11:85). A realm of appearances in which men present themselves to each other as outstanding whos, she asserts, has been absorbed by a determination of the human being as mere need-fulfilling labourer.

Because of her thoroughly anthropological perspective from the *animal laborans*, Arendt demonstrates no knowledge of the signal features of the Marxian analysis of capital. The cyclical movement of value as capital disappears beneath her focus on the cyclical "movement of the living organism", the "cyclical, life processes" that return "into the over-all gigantic circle of nature herself" (13:96). Since she conceives labour entirely in connection with the natural, biological life-process and its continual necessity to fulfil needs, she thoroughly misreads *Capital*, even to the point of confusing the biological reproduction process with the reproduction process of total social capital when she claims that "in the third volume of *Das Kapital* he [Marx] repeats that surplus labor beyond immediate needs serves the 'progressive extension of the reproduction process'" (13:99). If, however, capitalism is to be understood ontologically rather than anthropologically, it must be conceived as an historical constellation of value in augmentative movement under which human being itself is subsumed in an interplay of value-estimation that I have called the *gainful game*.[216]

Arendt's distinction between labour and work collapses in the modern capitalist world where the labourers labour, producing not only the necessities of life in a given society in a given time (Arendt's labour), but also fixed capital goods that build the infrastructure of a stable world (Arendt's

215 Cf. Eldred 2008/2011 Section 4 v) 'Aristotle on money and exchange—Money as a medium practically unifying social usages'.

216 Cf. Eldred 2000/2010 and *2.2.6 The private individual and private property as a mode of reified sociation: the gainful game (classical political economy, Marx)*

work). Furthermore, the distinction between labour and action, too, starts to leak when the character of labour as value-generating and being estimated as valuable is taken into account, because value is that phenomenon which comes about when performed labour (commodity products) and labour power itself (the living wage-earner, from production line work to top executive) are estimated and valued on the various markets through being *paid* for. Such payment is an indirect, reified valuing, esteeming and estimating of the labourers' (wage-earners') labour, which is a kind of indirect who-recognition for which wage-earners *vie*. This may be very far from the striving for "immortal fame" in the ancient Greek world through "speaking and acting", but the striving for reified estimation of one's worth in society through earning wages, is nevertheless akin in the sense that both amount to showing oneself off *as* who one is and being estimated and esteemed for this display of individual powers (cf. the next section). Hence Arendt's threefold distinction among human activities is only approximate and plausible, and beset by certain confusions.

Whoness and the gainful game

If Arendt's postulation of three distinct and fundamental kinds of human activity and three distinct determinations of human being itself is untenable, then, in particular, action and economic activity (which Arendt places under the rubric of labour and work) can coalesce. "Speaking and acting" through which "men" show themselves and show themselves off *as* who they are within the plurality of shared world are not separated off in a separate political or public realm. Rather, as Arendt herself concedes, the public realm includes also economic action: "exchange itself already belongs in the field of action and is by no means a mere prolongation of production" (29:209). Unfortunately, she does not take this thought further in order to bring to light how market exchange itself can be conceived as part of the action through men estimate and esteem each other as *who* they are. The exchange of commodity goods on the market is, namely, already an *indirect*, *reified* way through which, in particular, "men" display their labouring and entrepreneurial abilities to each other and estimate them through the products (including services) offered on the market. Not a word from Arendt on this aspect. The reason is that she neglects exchange-value as a phenomenon of mutual estimation and reified power play. Already with the phenomena of advertising and salesmanship, a kind of speaking and acting is seen to be inherent in economic activity as associated with realizing reified value in the money-form.

For Arendt, somewho's identity is who he reveals himself to be through speaking and acting in the shared world. She claims that this identity does not lie in the hands of the individual himself, but instead in those of others who are able to tell the life-story in retrospect. Who-identity is a narrative told by others about how the who in question acted and spoke in life, a story that comes to closure only with death. This is very much the third-person perspective on an individual assessed and estimated by the others. From the first-person perspective, I experience my *self* also from the resonance I hear from others in the shared world, whilst also being as self the source of spontaneous movement, i.e. action in Arendt's sense. If my identity is ultimately the story told about who I was after my death, then whoness is irretrievably out of my hands; my identity is defined posthumously by others. This is the aspect of the *striving for immortality* that Arendt underscores. Each who strives to anchor his identity in posterity's remembrance. My lived whoness, however, is intimately tied to my actions and choices in life, i. e. it depends on whether and how I grasp or fail to grasp the potential for existing open to me in my time in my particular situation, including choosing those with whom I am to intimately share my life. Out of this particularity I forge my unique singularity.

The playing field for identity as somewho is the shared clearing for self-presentation, which includes also economic activity. In the modern capitalist age, economic agents are

defined by the character-masks of the four basic income-sources that are the value-forms assignable to the economic players: wages, rent, interest and profit of enterprise, corresponding to the hired employees, the land-owner, the financier and the active, organizing entrepreneur, respectively. (cf. *2.2.6 The private individual and private property as a mode of reified sociation: the gainful game (classical political economy, Marx)*) These four figures are socio-ontological determinations of who one can be in a capitalist economy, occurring empirically in all sorts of mixtures and gradations.

Arendt neglects the economic power play among a plurality of economic players. In fact, as we have seen, she neglects the power play among a plurality of whos altogether.

Public and private realms?

Arendt develops her distinction between the public and the private realms from the paradigm of the Greek city-state in which the household was the hidden, private realm for the fulfilment of needs by women and slaves as a necessary precondition for the head of the household to be free to show himself off in the public realm (the agora) in a contestation among equal, free men. "The political virtue par excellence" (5:36) was therefore "courage", i. e. ἀνδρεία, literally 'manliness'. In this clearing of togetherness, men strive for "immortal fame", a striving which, Arendt claims, has become alien in the modern world where everybody is merely a consuming wage-earner ("jobholder" 5:31). For Arendt, the public realm is that of the "disclosure of the 'who' through speech, and the setting of a new beginning through action" (25:184) whereas the private realm is "the sphere of the household and family ... related to the maintenance of life" (5:28). She therefore grasps the crucial aspect of the distinction, namely, as that between *disclosing* oneself as *who* one is or *hiding* oneself in the privacy of the household. The play of disclosing and concealing who one is, however, cannot be tied down to separate "realms" or "spheres". Nor can the disclosure of who one is be restricted to "speaking and acting", as Arendt herself concedes when she writes that "men disclose themselves ... even when they wholly concentrate upon reaching an altogether worldly, material object" (25:183). This amounts to an admission that in modern *society*, too, which she marks off from the Greek city-state, there is who-disclosure in economic striving.

This shows up a weakness in Arendt's narrative, historical mode of presentation of her thoughts, for the play of showing off and concealing one is the essential feature of whoness itself, that is not tied to an historical paradigm. Rather, even when, as Arendt says, the Greek division between the private household and the public realm no longer pertains, and instead the household has come to be writ large as modern society, in which the economy (οἶκος), earning a living in the economy and economic management by the state become all-dominating, the play of whoness is not overcome historically, but assumes a new guise. It plays out now also within the *gainful game*, which is the socio-ontological structure underlying the modern market economy that remains hidden to Arendt.

Modern private intimacy offers a new setting for the play of revealing and concealing who one is to the intimate other which is different from the who-games the person indulges in out there in society when one must be careful to choose the right who-masks (personae) for the occasion. The games of intimacy between you-and-me are perhaps even a fourth kind of human activity besides Arendt's proposed (faulty) tripartite division of human activity into labour, work and action.

Despite the misgivings articulated in the above appraisal, Arendt is to be praised for placing the phenomenon of whoness as self-disclosure at the centre of her major work and also for putting her finger on the essential aspect of (personal) privacy, namely, the withdrawal from exposure to the public view, although who-games of revealing and concealing are played precisely also in public spaces, even before 'everybody'.

2.2.12 RECAPITULATION AND OUTLOOK

With the preceding section, we have concluded the presentation of the elements of a phenomonology of *whoness*, its relation to *personal privacy*, and marked personal privacy off from that of *private property*. A sketch of private property in the modern world in its essential value-structure has led to a determination of the essence of market-capitalist society as the *gainful game* of *reified value in movement*. All these preparations will serve us well when we come to consider today's world which is permeated by digital technologies of all kinds, and even increasingly enveloped by them. Whoness, privacy, private property each assumes a different character in a digitized world. Before being able to approach these questions, however, it is necessary to first provide a sketch of what the digital means, not merely superficially as a new kind of technology, but as a way in which the very being of the world is cast and presents itself. The following chapter will culminate in a concept of the *cyberworld* that will facilitate consideration of privacy in today's fast-emerging and consolidating digitized world.

2.3 DIGITAL ONTOLOGY

Michael Eldred

Here ontology is not to be understood in the insipid signification it has come to have in modern science, namely, as a complex taxonomy of terms and their interrelations in some subject area: "Ontologies therefore provide a vocabulary for representing and communicating knowledge about some topic and a set of relationships that hold among the terms in that vocabulary."[217] Rather here, the ontology practised still breathes in the inspiration from Aristotle's *Metaphysics* as an investigation into the being of beings in four distinct dimensions.[218] Whereas, however, in Greek philosophy, being itself was tacitly understood as standing presence, here being itself is overtly understood as coming-to-presence within three-dimensional time-space, and beings are likewise conceived temporally as that which comes to presence and presents itself in this time-space. Beings are the 'presents' that present themselves in time-space, either as present or as absent in two distinctive ways. But I am jumping ahead of myself by introducing at the outset a still unheard-of understanding of being that has been around for less than a century. So let me go back very briefly to the beginnings with Plato and Aristotle.[219]

2.3.1 FROM THE ABSTRACTION FROM PHYSICAL BEINGS TO THEIR DIGITAL REPRESENTATION

Plato famously located the being of beings in the εἶδος or ἰδέα or 'sight' or 'look' that a being presents of itself to human understanding. A being takes a stand in presence and presents itself in a well-defined sight. It can only be seen *as* a being through its 'ideal sight'. In Aristotle, the Platonic 'sight' becomes the μορφή or 'form' that is impressed on the material and brings it to a visible stand in presence *as* a being that can also be addressed by words.[220] As is well-known, however, Plato's metaphysical thinking was influenced by a close proximity to Pythagorean geometry; the visible geometric contours of a being that is present are akin to the 'sight' that a being presents of itself. The affinity of metaphysics and mathematics from the culmination of Greek philosophy is the beginning that will maintain its hold on Western thinking, and thus Western history,

217 Ontology Working Group 2002 http://www.cbil.upenn.edu/Ontology/#ontology.whatis This is in line with the prevailing understanding of ontology in analytic philosophy as "The basic question of ontology is 'What exists?'" (Chalmers 2009). Note also the developments in the area of the semantic web, which is based on such taxonomic ontologies; cf. Capurro 2006 that draws attention to the connection between the hermeneutics of texts and the so-called ontologies of the internet.

218 Very briefly, these four dimensions are with respect to i) the categories, ii) movement, iii) truth and falsity, iv) intrinsicality and contingency.

219 Cf. Eldred 2009/2011 or Capurro 2001 for an in-depth treatment.

220 Cf. Capurro 1978.

up to the present day with its own culmination in the digital dissolution of the being of beings. Only by understanding where the digital comes from in the history of Western thinking will it be possible to assess and critique present-day attempts to come to terms philosophically with the digital world (cf. in particular the critique of Floridi in sections 2.4.8ff).

Aristotle rethinks some of Plato's key insights in an alternative language. In particular, he thinks through the mathematical entities starting from physical beings. Both the geometrical and the arithmetical are the result of abstracting from physical beings which, for Aristotle, are beings that are subject to movement, i. e. to change or 'over-turning' (μεταβολή). Such abstraction is a separating-off (χωρίζειν) in thought that results in independent geometrical and arithmetic entities, namely, geometric figure and arithmetic number. A physical being has a place (τόπος) which Aristotle thinks as the 'skin' enveloping a physical being, thus enabling it to present itself in the space of presence. Separating off this skin and regarding it as something separate results in geometric figure, which therefore no longer has a place, although the points within the figure have position with regard to each other. A further step in separating-off or abstraction is to simply count the physical beings present: 1, 2, 3, etc. Number is both placeless and positionless, and it is also *discrete*, in contrast to geometric figure, which is *continuous* in the sense that all the points that go toward making it up hang together very tightly. This distinction has momentous consequences for the history of mathematics and mathematical science up to the present day, including in mathematical logic and quantum physics, in which disciplines there are still unresolved antinomies directly relating to discreteness vs. continuity.

An abstracted number is very different from the λόγος that is given to a being as its name (ὄνομα). The discreteness of words means that they are countable, and therefore each can be assigned a number. Any kind of text is a finite series of words, which may be characters, as in Chinese, or composed of letters, and therefore this ordered sequence can be replaced by an ordered sequence of numbers, where each number in the sequence stands for a definite word, words in any given language being regarded as part of a finite vocabulary on that language. If the words themselves are composed of syllables or individual letters, they can be further decomposed into numbers standing uniquely for individual syllables or letters. Hence, by virtue of its countable discreteness, any text at all can be represented uniquely by an ordered string of numbers. Numbering and counting result in full *determinacy* of presence.

The next step is that any number at all can be represented to the base 2, i. e. in binary code, because any counting number can be uniquely and determinately expressed as the sum of powers of 2, just as it can be expressed uniquely in the decimal system as the sum of powers of 10. In base 10, ten symbols are required to represent the base, whereas in base 2, only two, the binary digits or 'bits' 0 and 1, are required. Hence, anything that can be said 'logically', i. e. in words, can be represented uniquely and determinately in a finite, ordered sequence of bits which, although composed perhaps of billions of bits, remains countable and finite. The deep affinity between number and word can be called the 'arithmologos', which is discrete, placeless and positionless. Furthermore, due to its arithmetic character, the arithmologos is *calculable*.

2.3.2 MATHEMATICAL ACCESS TO THE MOVEMENT OF PHYSICAL BEINGS

The discrete, digital, arithmological representation of the logos in itself is not world-shaking, because performing arithmetical operations on a digital sequence as such is not all that useful. It first becomes useful when the logos is a text saying calculably how physical beings move in a calculation or computation (λογισμός).

To be able to do this, physical beings themselves must be cast as mathematically accessible, as Descartes lays down in his famous *Regulae*. This text may be regarded as the metaphysical blue-print for the modern age as dominated by the mathematical sciences. Geometric access to physical beings practised already by the Greeks was the first port of call, but geometric figure itself cannot be subjected to a calculus. Theorems in geometry rely crucially on the intuition of spatial figure that cannot be reduced to mere calculation. Therefore, the points of a geometrical figure had to be expressed in number to become calculable. The points thus lose their position, but, in exchange for this loss, they become arithmetically calculable – in Cartesian geometry.

On the back of advances in mathematics, the formulation of physical mathematical laws of motion could forge ahead into more subtle types of movement beyond the mechanical motion of physical bodies. Movement itself could be mathematized as energy regarded as a flow of particles, especially electrons.

2.3.3 THE MATHEMATICAL CONCEPTION OF LINEAR, CONTINUOUS TIME

Aristotle already conceived time as a number lifted off movement by counting in which a later now is counted after an earlier now. Time is cast as an endless sequence of counted nows in a row. With the discovery, or rather, the casting of mathematical laws of motion, this counted nature of time, that can be counted by the ticking of a clock, no long suffices because motion itself takes place continuously, and the Newtonian laws of motion are expressible as equations in continuous variables according to which the state of a physical system can be calculated at a later point in time given the initial state at an initial point in time. Hence time itself, must be cast as a continuous linear real variable t that occurs in the relevant equations of motion. The rate of change of a physical system can be calculated only by differentiating with respect to the continuous variable t. And so on. Mathematical calculability presupposes *continuous* linear real time, whereas the determination of time as a quantity is only ever a clock-time that is always *discrete*. This is a further antinomy that haunts modern physics.

Nonetheless, equations of motion written in terms of a continuous linear real variable t give Western humankind a hitherto unimaginable control over movement of many different kinds. Moreover, the totalizing tendency of the mathematical sciences is to cast *all* possible movement in the world, including social movement and change, in terms of (perhaps highly complex) effective-causal motion that can be mathematically calculated, today by stepwise calculations (algorithms) in computers, perhaps using statistical techniques to draw regularities out of masses of data.

2.3.4 OUTSOURCING OF THE ARITHMOLOGOS AS DIGITAL CODE

If the mathematical physical sciences have unleashed seemingly unbounded calculable control over all movement in linear time, this arithmological power over physical beings takes on a decisive new quality when these equations themselves are digitized in binary code that is then impregnated in its own electromagnetic matrix.[221] The digitization of texts may open possibilities of representing them not merely on paper but via an electromagnetic medium itself.

[221] It is crucial here not to confuse the generality of an electromagnetic medium with, say, superseded technologies such as magnetic core memory. Any medium for inscribing bits must take advantage of electromagnetic phenomena in the broadest sense of Maxwellian electromagnetic force-field theory. It is force-fields that are mobilized for inscribing, processing, transmitting and storing bits. An electromagnetic medium in the present context is not restricted to employing magnetism, nor is it to be understood only electronically, i. e. as the movement of electrons. A photon digital processor, for instance, still employs electromagnetic phenomena, since light itself is an electromagnetic phenomenon, but neither simply magnetic nor electric. Chemical bonds holding molecules together are also electromagnetic in nature.

Such an impregnated electromagnetic matrix, however, only becomes legible to a human being if it is shown on an electronic display. To achieve this, the mathematical laws of physics are required that allow a transformation of digital representation from ordered bits in an electromagnetic medium to the illuminated representation of digital pixels on a screen, and vice versa, to be calculated. This transformation is then put into effect by a physical process driven by energy, i. e. by the controlled motion of electrons.

The digitized, outsourced control over movements in the physical world comes into its stride in our own time. The mathematical scientific logos that encapsulates laws of motion of many different kinds can be employed to understand countless situations involving a change of circumstances of whatever kind, and this understanding can be written down in a *digitally coded text*. This digital code itself can then be outsourced to an electromagnetic medium where it is employed to process digital data fed in.

The mathematician, Alan Turing, must be attributed the ingenious insight that a (Turing) machine that can algorithmically process, i. e. compute, digital data fed into it, can first be fed with the program code that encapsulates the algorithmic rules for processing all the data that will follow in sequence on the endless 'tape'.[222] This is the Universal Turing Machine that stands at the portal of the digital age by serving as the mathematical blue-print for the electronic computer that is becoming more and more ubiquitous in more and more guises today.

2.3.5 THE PARALLEL CYBERWORLD THAT FITS LIKE A GLOVE

Cyberworld is the name not for some merely ontic-factual thing, but the existential-ontological name for the ontic-factual internet plus other interlinked networks *insofar as* this global technical thing also represents an (electromagnetic) *medium for the movement of digital beings* in which we human beings participate and through which we also steer, either directly, or indirectly through automatically executable digital code. This gives rise, say, to the possibility of robots, which are artificially 'animated' machines that, once programmed, have the source of movement within themselves, even though they need a current of electrons to drive them. The cyberworld, as the materialization of the digital cast of being, is an artificial world produced by outsourcing the arithmologos as (executable, automatic) digital code that moves in its own global medium. The cyberworld is populated by countless trillions of bit-strings that are either 'passive' digital data or 'active' executable program code. These two kinds of code copulate with each other in countless billions of Universal Turing Machines,[223] generating new bit-strings that continue to circulate throughout the cyberworld.

The various digital computing devices of all kinds can be linked electromagnetically so that program code instructions and data can be sent among many digital devices, each of which is basically a Turing machine. This network has been set up as the internet, a network among (inter) computing devices. The hardware for this network is dispersed physically all over the globe, allowing global cybernetic control and transmission of data of all kinds. Insofar, the term 'cyberworld' is justified, indicating a globe spanned by an interconnected electromagnetic medium enabling total digital control which, however, is exercised by a plurality of programmers and bits of executable code. Hence, the totality is splintered into many control centres. This cyberworld has human interfaces or 'windows' with the physical world, such as keyboards, graphic display screens, microphones, loudspeakers, keyboards, touchscreens, etc., that enable human beings to look into this digital world, input data and program code,

222 Turing 1936.
223 Cf. Eldred 2012b.

receive messages of various kinds output from it.[224] The cyberworld also has both passive-receptive and active-productive interfaces with the physical world, receiving data through devices such as cameras or thermometers, and producing controlled changes in the physical world, such as when a computer program controls traffic lights, or moves a robot arm on a production line, or changes the settings on a dialysis machine according to patient's current data which the program has analyzed.

Total cybernetic control in the cyberworld breaks down, or rather splinters, due to the *plurality* of users who can inject digital code into this digital world that is designed to subvert the envisaged effect of other code.[225] The digital movements designed to be controlled by a certain program code can be negated, neutralized, subverted or exploited by additional program code. Strife arises among the various digital programs designed to control certain definite movements. Computer viruses, Trojans, etc. are written and disseminated to countermand other pieces of executable digital code. Such power play played out in the cyberworld raises the spectre even of *cyberwar*. In this way, the cyberworld itself becomes a playground for the power play among human players. The global cyberworld fundamentally changes the power plays, because now so many players are playing, and the power itself is digitized and outsourced in automatically executing algorithmic code. This counteracts the other tendency of the cyberworld to bring under control movements of all kinds, including in the physical world, through clever digital code.

Cyberspace

The spatiality of the cyberworld is curious. People speak of cyberspace as 'virtual reality', but this term is not justified insofar as the cyberworld as a genuine medium has its own spatiality through which human being itself can navigate. The two essential characteristics of spatiality for human being are orientation and approximation (in the sense of 'bringing into proximity' or 'nearing'[226]). Since the cyberworld is 'inhabited' solely by digital code (passive data and active, executable program code) which is nothing other than outsourced calculating human logos of an arithmetic, algorithmic nature, it is a homogenous space whose places are specified purely numerically in a kind of mathematical vector space of finite dimensions. Each place in the cyberworld is simply a co-ordinate position specified as an n-tuple of whole numbers. These co-ordinates can also be given names and these names graphic interface representations which are called web-sites. The cyberworld can thus be navigated by human beings who take their orientation from the co-ordinate places suitably re-presented visually as a graphic 'site'. Behind these sites, however, is simply a string of digital code, i. e. a (usually very long) number enabling digital control. If necessary, one can also do without the comfortable graphic interface. From such sites, bit-strings can be brought into proximity by the human user. The human user thus moves in cyberspace 'as if' in a physical space, employing the same existential characteristics of orientation and nearing as in the physical world. This is only possible because digital code itself can be translated back into a graphic re-presentation that 'looks like' the physical world. To this extent, the term 'virtual reality' is justified, but the digital code behind the graphic re-presentations is 'really' distributed throughout the physical world on countless pieces of hardware (servers), and a user sitting in Helsinki 'really' can bring digital data on a device in Sydney into proximity on his own digital device.

Cybertime

What about the temporality of the cyberworld? Is there a peculiar cybertime to be distinguished from the time-space in which human being itself exists? Cybertime is

224 With inventions and refinements of the 'mouse' pointing-device, the graphic interface, the touchscreen, etc., Steve Jobs was a genius in understanding the importance of the 'handiness' of the interfaces between the human body and the materialized digital. On digital 'handiness' (Zuhandenheit) cf. Capurro www.capurro.de/floyd.htm, Capurro 1986 and Capurro 'Interpreting the digital human' www.capurro.de/wisconsin.html

225 Cf. Winograd & Flores 1986; cf. www.capurro.de/winograd.htm

226 Cf. Eldred 2009/2011, § 4.2.

the clock-time digitally registered automatically within the cyberworld of occurrences taking place within it. Every movement within the cyberworld is a change in digital bits of some kind or other. Each of these occurrences can be given automatically a time-stamp according to global clock-time (Greenwich time/UTC). Cybertime is thus a globally co-ordinated, digital counting of now-moments that can be used to date any occurrence in the cyberworld. Due to the cybernetic surveillance and control of all occurrences in the cyberworld, the *dateability*[227] of all occurrences is total, automated and indelible, unless the time-stamp data are deleted. Digital beings embedded in the global electromagnetic matrix are there 'forever' as long as the necessary electrical energy is supplied or the magnetic media are intact, and as long as they are not deleted by an electromagnetic force acting on the force-field that is the electromagnetic medium.

Time-stamped occurrences in the cyberworld are recorded by data that in themselves are timeless.[228] Only a human being inhabiting time-space with its three independent temporal dimensions is *in time* and can therefore also use time-stamped data to construct other digital beings, i. e. software, that employs these data for a definite purpose, e. g. tracking the progress of a postal delivery. By outsourcing the temporal understanding of the world to digital code, it seems as if this code itself were 'in time', but this is an illusion today often indulged in. In particular, any user's activities in the cyberworld are automatically registered as cyberworld occurrences, providing, on (human) recall, a complete timeline profile of where and when the user in question has been in the cyberworld. The digital trace of users' movements is one important aspect of being-in-the-cyberworld arising from its totally cybernetic character. In the physical world, the trace of an individual's movements can never be so complete. Hence other individuals, companies and the state can construct temporal profiles of users' movements, either of specific users or of types of users, depending upon how specific the time-stamped data are.

With respect to the temporal dimension of the future, dateable cybertime proves itself to be invaluable by providing endless amounts of time-stamped data on digital occurrences in the cyberworld that can be analyzed or 'mined' using mathematical statistics to discover regularities and correlations which, in turn, can be extrapolated into the future. In this way, future occurrences in the cyberworld can be predictably modelled in linear time, especially with a view to uncovering future *trends*. Where the movements of many users in the cyberworld are available as time-stamped data, mining these data is a valuable tool both for the state and private companies as we shall see in more detail in the next chapter. The attempt to mine and extrapolate the plethora of time-stamped data is based on a *linear, one-dimensional* conception of time.

With this section, the crucial concept of the cyberworld has been developed, which will enable us in the next chapter to bring together a phenomenology of whoness focused specifically on personal privacy and private property, on the one hand, with today's specifically digitized nature of being-in-the-(cyber)-world, on the other.

2.4 DIGITAL WHONESS IN CONNECTION WITH PRIVACY, PUBLICNESS AND FREEDOM

Michael Eldred[229]

The two preceding chapters have provided a sketch of a phenomenology of whoness with special regard to privacy, publicness and freedom as well the rudiments of a digital ontology that allows today's cyberworld to be seen as the

227 Cf. Heidegger SZ 1927, § 79 and Eldred 2011a, § 6.
228 Cf. Eldred 2012b.
229 All sections of this chapter are the final authorial responsibility of Michael Eldred, apart from section 2.4.7 by Rafael Capurro.

consummate way in which the digital cast of being comes to presence and presents itself today. The task for the present chapter is to bring these two strands together so that specifically *digital* whoness, privacy and publicness come to light.

2.4.1 DIGITAL IDENTITY – A NUMBER?

Who someone *is* is a way of presencing in the world. To be somewho means to be a *self* which comes about through an individual's *identifying* with, i. e. adopting as his or her own, certain chosen possibilities of existing that shine back from the world. On the other hand, we have seen that the digital cast of being, i. e. the way in which all beings shape up and present themselves as decomposable into bits, precipitates today in an artificial cyberworld in which digital beings circulate. The human interfaces with the cyberworld make it fit like a glove, so that the borders between being-in-the-cyberworld and being-in-the-physical-world become increasingly blurred. 'Like a glove' here is neither a metaphor nor a simile, but an English turn of phrase that points to and says how human bodiliness fits with the artificial cyberworld. The two intermesh seamlessly into a unified everyday being-in-the-world. What does this signify for individual selfhood, i. e. individual identity?

The digital beings 'inhabiting' the artificial cyberwelt are nothing but strings of 0s and 1s, i. e. a finite binary number. These binary numbers, however, are 'magical' in the sense that they unfold into all sorts of data or information about the world, on the one hand, and, on the other, into executable program code that processes data to bring forth calculable effects both within and without the cyberworld. As far as the human user or denizen of the cyberworld is concerned, the cyberworld presents itself to him or her through the various interfaces that today have been well-adapted to the human body and mimic the physical world. Such interfaces are technical, requiring a technical device. This device itself is assigned a number automatically (e. g. IP address) by the cyberworld; it is identifiable through this number, which may be combined with other numbers such as location and time co-ordinates. The human user of a digital device interfaced with the cyberworld is willy-nilly identified with this device's number so that, in a certain way, the user's identity itself becomes this number as far as his or her presence in the cyberworld goes.

The cyberworld denizen both sends messages through and receives messages from the cyberworld via the convenient technical possibilities put at her or his disposal by the programmers.[230] Such messages are themselves digital beings. A cyberworld denizen can call up data from all over the world, according to his or her interests, which are a reflection of personal identity, i. e. of who this individual understands him- or herself to be in the world. A cyberworld denizen can also present him- or herself as who s/he is by posting data at some site within the cyberworld. These data, of whatever kind (text, image, sound, video) are *identified* with the individual posting them, who may use a pseudonym.

The cyberworld also offers a space for individual whos to present themselves as who they are by placing bit-strings (mostly data) in and sending them through the cyberworld. With its visual and audio interfaces, the internet has opened untold possibilities for self-presentations of all kinds which can be called up globally by anyone.

Another aspect of finding one's self in the internet age is that, due to its global reach, the cyberworld reflects many different possibilities of living in the world, from all the world's different cultures. Ease and cheapness of access to the internet for billions of people open up a vast space in which to find one's self, thus perhaps causing friction with the expectations within the ethos of a given culture.

230 Cf. Capurro & Holgate 2011.

2.4.2 DIGITAL PRIVACY: PERSONAL FREEDOM TO REVEAL AND CONCEAL

As discussed in Chapter 1, there are two basic kinds of privacy: personal privacy and the privacy of property. The former has to do with disclosing and concealing *who* one is, whereas the latter concerns access to, use and disposal of various kinds of property. In this section the focus will be on the former, and in the next on the latter.

It is paradoxical that to be somewho implies a striving for *showing* oneself off *as* who one is in the world, the very opposite of a withdrawal into hiddenness. These are games of self-presentation, of pretending to *be who* one is through the adoption of one mask rather than another, which is by no means a matter of mere pretence, because to be somewho at all, some kind of *fitting* mask or other must be adopted with which one genuinely identifies or with which, through sheer unconscious habit, one has unwittngly identified. With a mask of self-identity, no self-presentation at all. Showing off who one is can go through a gamut of gradations, even to the point of such diffidence or modesty that one would rather not put oneself on show at any price, but instead lead a quiet, undisturbed life in seclusion. With the advent of the cyberworld, the possibilities for revealing who one is multiply exponentially, and the possibilities of tracking somewho's movements in the matrix of the cyberworld are immense, since every movement leaves a digital trace embedded in the matrix. In this sense, it is virtually impossible to remain hidden as who one is in the cyberworld. One has to go to extraordinary technical lengths to cover one's tracks in the cyberworld, an effort most people do not want to make, if only because they have no clue about how to achieve it technically. Since the cyberworld, by its very cybernetic nature, offers such strong technical possibilities of tracking anyone's movements in the cyberworld, including any data an individual deposits on any public site within the cyberworld, issues of personal privacy come to the fore.

One way – perhaps the *key* way – of concealing who one is in the cyberworld is to encrypt one's data. Another is to keep one's data, whatever they may be, at a site in the cyberworld to which access is limited and controlled. Since, within the cyberworld, one is (identified with) one's data, data encryption amounts to a powerful way of veiling one's identity and one's movements in the cyberworld. *Encryption* itself is a technology relying crucially on mathematics, especially pure number theory of the prime numbers and, more recently since the advent of the *idea* of quantum computers employing quantum decryption algorithms, other cryptographic theories such as code-based, hash-based, lattice-based, multivariate-quadratic-equations and secret-key cryptographies.[231]

Private sites in the cyberworld, to which access is controlled, must go hand in hand with encryption techniques because data must be transmitted back and forth between a user and a private site in the cyberworld (that is, a certain server in the internet). Concealing who one is, i. e. maintaining one's privacy, thus becomes a matter of digital technical finesse. Private sites in the cyberworld are protected by passwords or some other technical means such as card readers or iris scans. These techniques work according to the principle of matching two parts of a symbolon in the Greek sense, like a key with the lock, which now are simply two bit-strings that must match to gain access to a site where certain data can then be 'seen'.

2.4.3 PROTECTION OF PRIVATE PROPERTY IN THE CYBERWORLD

The other aspect of cyberworld privacy, which must not be confused with personal digital privacy, are the digital, cyberworld aspects of private property. This concerns both digital data that are *themselves* private property and digital data *about* private property. The focus here will be on the former. Protection of digital private property has an

[231] Bernstein et al. 2009, pp. 1, 17.

eminently economic aspect and importance. Insofar, it concerns the gainful game, as introduced and outlined in *2.2.6 The private individual and private property as a mode of reified sociation: the gainful game (classical political economy, Marx)*. In the area of personal privacy, digital private property concerns a person's private life-world which needs to be protected, i. e. kept hidden, by limiting access to personal digital data on that person, an issue discussed in the preceding section. Here, therefore, we will concentrate on the economic aspects of digital private property which, at the same time, are then of juridical importance.

Every player in the gainful game is an income-earner of some kind. The aim of involvement in the economic game is always money-related, money itself being the reification of value whose movement through its various forms *is* the capitalist economy. Each of the four basic income-types is the price of buying or hiring an income-source. The reification of value as money and price is *arithmetically quantitative*, and thus discrete, which enables easy digitization and hence also almost unlimited scope for calculation, starting from bookkeeping through to models of whole economies running on super-computers. The movement of a capitalist economy, which is, in its hidden essence, the movement of value in myriad circuits of capital, can be captured mathematically and hence also digitally, and that in countless phenomenal forms such as supply control, logistics, personal finances, financial accounts of companies small and large, market transactions of all kinds from consumer retail through company turnover to stock exchange transactions in highly derivative products. Money itself can become digital, i. e. a jealously kept bit-string kept in an electromagnetic purse. Payments can be made in the cyberworld simply by transferring a bit-string for a certain amount from one digital purse to another.

Private property in the form of *personal* income also has a connection to personal privacy because the individual income-earner is also an individual spender, i. e. a *consumer* (along with family members who help spend what the breadwinner has earned). Consumption is an important, if superficial, aspect of personal identity-formation and -cultivation insofar as consumption reflects how an individual shapes his or her private world and understands him- or herself as some particular who from among the countless self-defining possibilities on offer, thus marking him- or herself off as who from others. Being a consumer, however, brings an indivdual into contact with firms selling consumer goods. The firm itself may be located in the cyberworld, giving rise to *digital retail commerce*, i. e. *e-retailing*, on the digital retail market, which is one kind of market among many that exploits the medium of the cyberworld.

Corresponding to the four basic kinds of income-source property as discussed in Chap. *2.2.6 The private individual and private property as a mode of reified sociation: the gainful game (classical political economy, Marx)*, it can be asked what their digital cyberworld counterparts are, viz. what is a digital labourer, what is digital land, what is digital money-capital and what is a digital enterprise. Let us consider each of these in turn.

Since the labourer (*wage-earner* of any kind) as a living human being is also the bearer of (the right to) life and liberty, this income-source is not for sale (although its labour power, whatever it may be, can be *hired* out and expended in labour of some kind or other), and also cannot be digitized, despite the suggestive analogy with robots or, perhaps, avatars.

Land in the cyberworld (*cyberland*) can be regarded simply as a binary number, like anything else in the cyberworld. Digital land is nothing other than a numerical address (or several) in the 'universe' or cyberspace of all possible cyberworld addresses. Such addresses are generally called IP (Internet Protocol) addresses which are an n-tuple of integers, hence countably finite and also rational in the

mathematical sense. Having an address, position, *digital location* or *digital place* in the cyberworld is the precondition for posting any digital beings there (data and executable code), and for any other digital beings (such as a user's command) reaching it.

Although digital locations are merely a binary number, this number is associated with a (domain) name, which is of crucial importance for presenting who one is in the digital world, whether it be an individual person or a company. Therefore, certain names and their associated cyberworld locations (domain names) are jealously guarded, especially for commercial reasons, and therefore command a price, which may be called *digital (or cyber-) monopoly ground-rent*.

A *digital business location* must have a shopfront where prospective customers, who may be consumers or other businesses, can enter. Hence some of the digital code at that location must be made accessible to prospective customers, i. e. it must be public, whereas the backroom remains private. A significant issue in private property rights concerns the data and the data track that prospective customers or simply visitors to a commercial digital business location leave behind. To whom do these data *belong*, and to whom and for what purposes may they be *employed* and *disclosed*? Issues of personal privacy here clash head on with commercial private property interests. Hence the importance of clearly having in view the two different primary phenomena of privacy.

The equivalent of *means of production* and *means of circulation* in the cyberworld is the software (executable code) kept at the cyber-business location to generate or make available *digital products* for customers. Digital products can consist of data of various kinds that may be legible (fairly) directly (e. g. a journal or 'newspaper' article, an e-book) or more indirectly (e. g. the audio file of a song, the video file of a movie which must be processed by the appropriate software in the appropriate hardware) or executable digital code (software of any kind for both personal entertainment and business purposes).

Cyberworld banking is a case in point where secure intercourse with the bank is paramount. Money itself takes the form of a bit-string recorded in a customer's account from which withdrawals can be made by transferring digital data across the cyberworld to a recipient's own bank. Commercial transactions in the cyberworld thus combine aspects of both personal privacy and private property. Personal privacy is involved insofar as the individual making transactions does not want this to become common public knowledge.

A special problem arises with regard to *commodity products* that are themselves digital, such as texts, music, film and software, because these are simply (perhaps extremely long) bit-strings that can be copied in the electromagnetic matrix almost without cost, i. e. given that one has a digital device of some kind for storing bit-strings. The *production* of such a bit-string may have cost an enormous amount of labour (e. g. years spent by an author writing a book or by programmers developing a piece of software such as a game), technical means of production (e. g. a recording or film studio), invested money-capital, ground-rent for a production site, but the *reproduction* of the digital product costs almost nothing.

Digital loan-capital in the cyberworld is simply money loaned via the medium of the cyberworld. An individual or company with credit from a bank or some other lending institution can call down credit lines online, or an online bank account is supplemented with an additional balance over which the lender can dispose.

Another aspect of digital privacy concerns the relationship of individuals and companies to the *state*. This concerns not only surveillance of an individual's or a company's movements in the cyberworld, but also, and especially, the disclosure of digital financial movements for *taxation* purposes.

2.4.4 CYBER-PUBLICNESS

The global electromagnetic matrix that we have dubbed the cyberworld (in preference to 'internet'), provides places to bit-strings of all kinds that can be inscribed in it, where they can also change co-ordinate places, i. e. circulate in this vector space. Those bit-strings that can be taken in and understood without further ado by human beings, such as written texts, images, audio recordings, digitized movies, etc., may be called *(immediately) intelligible code*, in contrast to executable digital code (programs, software, apps, routines, algorithms) and *processing data* that are 'read' only by digital programs to produce automatic effects that are not immediately taken in by human beings. For the sake of clarity and simplicity, we introduce the distinction between *digital messages*, which are (immediately) intelligible code circulating exclusively among human beings and legible to them, and *digital signals*, which are processing data sent to a digital device for processing, from either another digital device or some physical source (e. g. incident light, ambient air).

In this section, the focus is on those digital beings, immediately intelligible code or digital message, that human beings can take in and understand and appreciate, starting with written messages, but including of course also photos, music and film. Such messages can be either private or public. Private messages are addressed and circulated to those friends and acquaintances who are part of one's own personal life-world; they may be posted at a location in the cyberworld to which only these friends have access. With such messages back and forth, friends show themselves to each other *as* who they are, thus sharing a private world. They may indulge in shows of self-presentation that are not intended for the world at large, in which they adopt other masks for their public personae. An important aspect of personal privacy as a valued aspect of living one's life has thus become the protection of private messaging in the cyberworld against intrusion of all kinds, whether it be from other persons, from companies or the state. Such messaging is an aspect of the play of revealing and concealing who one is oneself, which amounts to the play of revealing and concealing one's own private life-world. Having control *oneself* over this who-play of disclosure and exposure is today an important issue for personal freedom which is very difficult because the cyberworld by its very nature enables digitized control *by others*.

Conversely, the cyberworld offers hitherto unknown potentials for presenting oneself as who one is to others in general, i. e. to the public, since an individual can post almost any digital message at some location or other in the cyberworld or send it through the cyberworld to many recipients, as with a public e-mail discussion. There is thus a specifically *cyber-publicness* based on the circulation of digital messages freely through the cyberworld to 'anyone who'll listen'. This cyber-public-sphere already encompasses the entire globe, providing a platform for anyone to present themselves as who they are through digital messages sent out into the cyberworld.

Digital messages of all kinds have to be taken in and interpreted in one way or another by others, giving rise to *differences of opinion*. This is the *controversy* related to what a message discloses about the world, no matter whether it be a trivial matter or one of great import. Insofar as it is open to everybody, the cyberworld is a neutral medium that lets both shallow and deep messages through.[232] There is always *strife* over truth, especially over the deeper truths of the world. Consumers expressing their opinions about products they have used (e. g. a stay at a certain hotel) may disclose a useful truth for other consumers that has very little to do with the identities of those posting such consumer-goods' assessments. The artificial medium of the cyberworld offers analogously the same possibilities for exchanging or publicizing messages

[232] Cf. Eldred 2011b.

of all kinds as the other media do. Its easy and cheap accessibility to everybody draws praise for its so-called 'democratizing' potentials.

The circulation of digital messages in the now global cyberwelt contributes to the formation of a *global public opinion* that is not uniform, but marked by segments and a back and forth of opinions on issues of the day. This global public opinion goes hand in hand with *global moods* that permeate the global medium of the cyberworld atmospherically, ranging from uplifting to downcast through all possible gradations from momentary euphoria through to despondency.

2.4.5 FREEDOM IN THE CYBERWORLD

The cyberworld frees itself first of all

The cyberworld is the artificial, global, electromagnetic medium for the movement of bit-strings of all kinds through it. Freedom of movement relates first of all to bit-strings themselves, which are free to move in the same sense employed in physical dynamics for the motion of physical bodies. Freedom of movement for bit-strings thus signifies a technical enablement of their motion through the cyberworld. Freedom in the cyberworld is therefore, in the first place a freedom for the cyberworld itself to unfold its digital powers of control over changes within and without the digitized electromagnetic matrix. The cyberworld unleashes its cybernetic powers of control upon the world as a whole. Such bit-strings may be message data for communication between and among human beings, or they may be processing data, or they may be program code itself, including malicious executable code or 'malware'.

'People' are also very enthused by the possibilities of working from home or from shifting, self-chosen workplaces that have opened up through the technologically enabled option of sending bit-strings through the cyberworld. People, or at least some segments of the workforce, are less tied to specific workplace locations and have become freer in that sense. The movement of bit-strings can substitute to some extent for the movement of human bodies by means of transportation. Business communications have become quick, easy and highly mobile, not just for personal communication, but also for sending business data back and forth for informational purposes or to be processed further. From a personal and business point of view, the cyberworld seems to enhance our being in the world. As a drawback, there is only the danger that privacy, in the double sense developed in this study, will be violated, such as when the personal data of private persons are 'hacked' or business secrets stolen from internal company data-servers.

But there are deeper issues of freedom here relating both to technology itself and to the economic mobilization of the globe. Digital technology implemented in the cyberworld seems to be for the convenience of its users, to make their lives easier, but the converse is also the case: the more digital technologies are incorporated into everyday lives, the more living becomes dependent upon these technologies. Mobile telephony, for instance, seems to be a boon for humankind, but it also turns human beings into the appendages of their mobile phones and other mobile digital devices to receive all kinds of digital messages from voice messages through text messages to photos and videos. The all-surrounding cyberworld grafts itself onto the everyday world as a natural part of it which 'nobody' can do without. The movements of bit-strings through the cyber-matrix starts to dictate the pace of everyday life wherever the cyberworld pervades.

'Surrounding cyberworld' is a synonym for so-called '*ambient intelligence*' that is one of the emergent technologies which will immerse people in an environment 'populated' by networked digital devices into which human intelligence has been outsourced, thus making the devices themselves seem intelligent. 'People' develop an 'intimacy' with their ambient cybernetic devices

that control certain aspects of their everyday lives and they thus become dependent on them for shaping their lives and directing their lives' movements.

With regard to the public media, especially the speed with which digital messages are disseminated throughout the cyberworld generates the illusion that the latest news bit-string is the best and most important. Under the impact – or onslaught? – of the budding cyberworld, the news media are sucked increasingly into the vortex of the 24x7 news cycle.

The gainful game unleashes its freedom in the cyberworld

There is also an intimate connection between the fluidity of the cyberworld and the inherent tendencies of a global economy to mobilize everything and everybody gainfully. As we have seen (*2.2.6 The private individual and private property as a mode of reified sociation: the gainful game (classical political economy, Marx)*), the capitalist economy can be conceived as the movement of value in self-augmenting cycles. Money-capital is advanced with the expectation that it will return augmented with profit after all costs have been defrayed. All the various sorts of income-earners are players in this now globalized gainful game. The cyberworld as a powerful technology provides the opportunity i) for massive cost reductions in all sorts of ways, especially through automating production and circulation processes and ii) for increasing the rate of turnover of capital, and thus profits, especially by facilitating communications with employees, customers, suppliers. In particular, the cyberworld enormously enhances the movement of money as cyber-digits. Transactions of all kinds can now be done more speedily, including receipts from customers, payments to suppliers and employees, loan transactions with banks, and so on, thus reducing turnover-time. Today's banks have profited enormously by the introduction of digital automation, saving labour costs, cutting workforces and pushing the costs of transactions onto customers, who now have to purchase the digital equipment to communicate with their bank accounts and learn the ins and outs of their banks' software without the banks incurring any training costs.

Work productivity can increase through automated processes outsourced to the cyberworld and especially through the ease of communication with employees anywhere, anytime that turns employees themselves tendentially into appendages of their digital messaging devices, on constant stand-by for instructions from their superiors. An important aspect of the protection of personal privacy is to keep in place barriers to employees' becoming permanently contactible through the cyberwelt, at their employer's, business associates', customers', etc. beck and call.

Hence it can be seen that the gainful game can be played in and through the cyberworld which, as a global medium, can lubricate and speed it up. The gainful game and the cyberworld are affine, and because the latter is becoming more and more ubiquitous, the players can be drawn more tightly into the gainful game's play. One could say that the cyberworld is an excellent medium for the *freedom of the gainful game* itself, which is dissociated from its pawns, the income-striving players themselves, and under the control of nobody, especially not within the grasp of state controls or subject to a wished-for 'primacy of politics'.

Human freedom in the cyberworld

In view of the freedom enjoyed by the cyberworld to unfold its potentials and the freedom of the gainful game to extend its reach and intensity, both of which rely on a restricted meaning of freedom as a freedom to move, it has to be asked what *human* freedom in the cyberworld means. In view of the above, it would seem to be ambivalent because, apart from being encroached upon by the cyberworld, human lives also are enhanced by the convenience it affords, in much the same way as Adam Smith refers to the "conveniencies of life". The sheer cybernetic powers of the cyberworld offer the potential for shaping one's own life in many hitherto inconceivable ways including especially the possibilities for sharing

one's world with others either privately or publicly. Keeping in touch with family, friends and acquaintances globally becomes an easy matter of course. The possibilities for presenting oneself in the public space increase exponentially. Kant's community of scholars, for instance, becomes less exclusive through the ease of communicating and publishing via the cyberworld. Institutional power to play the role of gatekeeper, with regard to which scholar or thinker has something worthwhile saying, lessens, and along with it peer pressure.

We turn now to consider alternative approaches to issues of privacy in the cyberworld.

2.4.6 ASSESSING TAVANI'S REVIEW OF THEORIES AND ISSUES CONCERNING PERSONAL PRIVACY

Private life-worlds as considered in *2.2.4 The question concerning rights: personal privacy, trust and intimacy* are prior to privacy conceived as "physical/accessibility, decisional, psychological/mental, and informational" as discussed by Tavani,[233] who provides a review of various theories of personal privacy under these headings. *Physical privacy* is a crude criterion because a private world cannot be tied down at all physically, and indeed, the very term "physical" (res extensa) is metaphysically loaded vis-à vis the 'psychic' (res cogitans). Rather, personal privacy is a social phenomenon. Not even the privacy of private property (cf. *2.2.5 The private individual, liberty, private property (Locke)*) can be conceived simply as restrictions to or control over physical accessibility, since use and disposability also come into play. Personal privacy need not imply a physical isolation at all, but 'merely' the hiddenness of one's affairs, even in public. Both "access to persons (and their possessions)" and "informational privacy" confuse two aspects of privacy, namely, personal privacy, which is a matter of disclosing or concealing a personal life-world, and the privacy of property, which is an issue of access to, and use, disposal and transfer of property.

Decisional privacy is a misnomer for the individual existential freedom to cast one's self, thus shaping one's own life-world, which is deeper than and provides the existential-ontological ground for making decisions. Decisional privacy is linked to an individual's having *control* over access to (ontic-factual) information about him which, again, is an aspect of personal privacy in the sense of being able to withdraw one's personal world from view to others and of being able to choose those to whom one wants to reveal and share one's own personal life-world.

Psychological privacy proceeds from the notion of the encapsulated subject with a psyche 'inside' the body (this bodily location usually being imagined to be, more specifically, the head), and thus remains captive to subjectivist metaphysics with its notions of consciousness generating representations of the outside world inside the head. It is the obvious counterpart to physical privacy within metaphysical thinking. If psychological privacy is to mean non-intrusion into a subject's mind, then it is impossible anyway, because, speaking from the phenomena themselves, there is no encapsulated subject and the mind is always already out there in the world where it is subjected to various influences, including attempted manipulations or prying. The human psyche *is* simply the openness to being-in-the-world.

Informational privacy, finally, is a superficial misnomer for the concealment of a personal world itself, i. e. that not everything about a personal life-world be exposed to public knowledge. If the focus is on "information", which is kind of entity, then it would seem that personal privacy would be protected by protecting data "both stored and communicated",[234] which, in the same breath, are[235] regarded as

233 Tavani 2008; cf. *2.2.10 Privacy as protection of individual autonomy – On Rössler's The Value of Privacy.* Interestingly, although Rössler has a somewhat similar categorization of types of privacy, Tavani does not mention her book.

234 Tavani 2008, p. 139.

235 Here we do not go along with the ongoing degradation of the English language, as practised by Tavani, by treating words with Latin plural endings, such as 'data' and 'media', as singular nouns.

a person's private property, which is here not the issue and from which personal privacy should be conceptually distinguished, but most often isn't. Personal privacy is invaded also, say, when rumours are circulated about an individual's private life, and data and information capture only the *third-person* aspect of an individual as a what, not as a who. Personal privacy can be violated also in a *first-and-second* person encounter between *you-and-me*, when you overstep the bounds of what I would freely reveal to you about who I am, i. e. about my own life-world. Such first-and-second person aspects of the phenomenon of personal privacy are necessarily overlooked by theories of privacy that are in search of 'objective' criteria instead of taking the play of revealing/concealing in the world as the hallmark of personal privacy.

The false lead of conceiving personal privacy as informational privacy, which has been blindly followed by today's debate on privacy and the internet, goes back to Alan Westin, who lays down that "privacy is the claim of individuals, groups or institutions to determine for themselves when, how, and to what extent information about them is communicated to others".[236] Even the broader definition of privacy offered by Hauptman et al., "Generally, we can state that privacy is closely related to the concept of intimacy including physical integrity, but there are a lot of other dimensions of privacy (spatial, emotional/inner life of a person) that privacy incorporates",[237] misses the concealment of a personal self's life-world as the kernel of personal privacy. Moreover, in its captiveness to subjectivist metaphysics, it confuses what is called the "emotional/inner life of a person" with a mooded life-world that is not 'inside' a person at all, but 'out there'.

Tavani discusses also Moor's "restricted access/limited control (RALC) theory" of personal privacy that at least has the merit of introducing privacy "in a *situation* with regard to others",[238] rather than merely the privacy of information or data. Situations only come about in a world. A world affords both concealment and disclosure of a situation. Moor makes the distinction between "natural privacy" and "normative privacy". Properly speaking, natural privacy refers to the play of concealment and disclosure that any who plays in the world.

Tavani also discusses issues of employee privacy, especially that of surveillance of employee activities through the deployment of digital technologies that can automatically record employees' movements in the cyberworld, such as e-mail correspondence or duration, or even content, of telephone conversations.[239] Here there is a clash between personal privacy and the privacy of private property insofar as the employee has hired her or his labouring powers to the employer for a specific job and therefore has an obligation, within limits, to carry out employers' instructions and perform duties within the job description. Within the terms of the employment contract, the employee has a right (and even a duty in the case of a public company) to supervise and monitor an employee's activities, but how far does this right extend? Digital technologies make it easy and cheap to check on what employees are doing, e. g. if they are wasting company time with personal activities, but such surveillance is also an infringement of *trust* in employees and also an invasion of personal privacy insofar as employees also have to manage their private affairs from the workplace. Where is the line to be drawn between *trust* and *control*?

The employer also has an interest and a right to monitor work *efficiency* as an aspect of measuring cost-productivity, but here, too, limits must be drawn. Measuring the duration of telephone conversations or the number of keystrokes per

236 Westin 1967/1970, cited by Hauptman et al. 2011.
237 Hauptman et al.2011.
238 Moor 1997.
239 Cf. section 2.6.

minute an employee types may be useful for measuring work efficiency, and easily implementable, but these practices are also repugnant in the sense of reducing the employee to a mere efficient agent of the employer's overall work organization. The interface between personal privacy, which is an important aspect of human freedom and dignity, and the private rights of private property becomes rich in conflict in the case of employees and employers, since employees are necessarily in close, live contact with their employers via the organizational hierarchy and, within limits, must do their employers' bidding. This perpetual *power struggle* is not simply an issue of personal privacy, i. e. of the extent to which the movements of employees are revealed to employers, but is embedded in the larger issue of employer-employee relations, which brings into play questions of private property rights, personal trust vs. supervision, human dignity and the freedom to be the responsible 'master' of one's own life-movements.

Tavani cites Regan's (1995) argument for privacy itself as a social good in terms of its being valuable for the "democratic political system" which, of course, begs the question as to the value of democracy as a form of government that must be justified, if at all, in the context of a clarified philosophical conception of human freedom. This has been a principal concern of political philosophy since Locke, with Hegel's *Philosophy of Right* being a certain culminating point, in which a concept of freedom is at the core, serving as the touchstone for assessing how a social order with its state can be compatible with freedom. Values are not merely "goods", but must be anchored in an ethos, a customary way of life that is held dear by people sharing a world with one another (cf. *2.2.3 Values, ethos, ethics*). In any case, privacy as an individual freedom to conceal or reveal a personal life-world does not have to justify itself to "society", but rather, society as a way of sociating and living with one another has to justify *itself* as compatible with freedom, which can never be dissociated from its core: individual freedom since it is in the first place human individuals who are the points of origin for their life-movements, free or otherwise.

2.4.7 AN APPRAISAL OF NISSENBAUM'S *PRIVACY IN CONTEXT*

Rafael Capurro

Helen Nissenbaum criticizes the private/public dichotomy as a presupposition for the idea that making personal data public means that such data can be used by anybody for whatever purposes without people being aware of it and/or giving their consent.[240] She is aware that, although it is "both unrealistic and unreasonable" to strive for protection of privacy in public, it makes sense nevertheless to exercise control over what one exposes for observation.[241] This distinction provides the basis for mechanisms of intellectual property such as patents and copyright. If the realm of the private is conceived as divorced from the public sphere, then the problem of privacy in public has no meaning whatsoever. As Nissenbaum remarks, this dichotomy has influenced the philosophical discussion by placing values such as "autonomy, liberty, personal relationships and trust" on the side of the private sphere alone.[242] Obviously, such a conception is the heritage of modernity and its view of the self as an encapsulated subject separated from the outside world. This separation gives rise to the right to privacy in the sense of a right to control information in an area strictly separated from the public realm, whose content may vary in different social and cultural settings. Commercial no less than political interests are particularly amenable to such a dichotomy, regarding any restriction of their actions with private information in the public realm as an unacceptable restriction of (their)

240 Nissenbaum 1998.
241 Nissenbaum 1998, p. 32.
242 Nissenbaum 1998, p. 9.

liberty. Nissenbaum calls this view of privacy from the perspective of liberty as the "knock-down argument".[243]

On these premises Nissenbaum develops a new conception of privacy based on what she calls "contextual integrity", a concept that she considers to be "the same idea" as that proposed by Jeroen van den Hoven, who uses the term "spheres of access",[244] as well as Michael Walzer's "spheres of justice".[245] Personal information in the public sphere is not "up for grabs", where no norms of privacy apply.[246] Obviously, the defenders of "data aggregation" and "data mining" are not interested in "contextual integrity". According to Nissenbaum, by taking information from one context into another, persons themselves are concerned. She points to "wide-ranging" individual values "such as autonomy, liberty, individuality, capacity to form and maintain intimate relations, mental health, creativity, personal growth; as well as social values such as free and democratic society".[247] She writes, "The picture of a person that a profile provides can, for the reasons given, be broad, deep and traverse time. These pictures may be rich enough to reveal aspects of an individual's character, to ground predictions about their propensities, and even suggest ways of manipulating them".[248] Nissenbaum's conception of privacy as dealing with the personal integrity of the self is related to Alan Westin's notion of "personal autonomy"[249] and Ruth Gavison's view of privacy as promoting liberty of action.[250] She refers also to Jeroen van den Hoven for whom the privacy of persons, which he calls "moral identification," is what is missing "when personal data are piled up in our databases and persons are represented in administrative procedures".[251] Moral identification "presupposes knowledge of the point of view of the data-subject and a concern with what it is for a person to live that life" (ibid.). Following the idea of the modern "liberal individual", van den Hoven considers privacy as a kind of "moral time out" for "moral reflection and self-improvement".[252] This view of the moral self is understood as related to the Aristotelean ethics of self-improvement.[253] But the modern categories of morality and legality no less than the idea of the modern self as detached from the world cannot be identified with the Aristotelean formation of individual character (ἦθος ethos) nor with the relationship between the individual and the *polis*.[254]

In her recent 2010 book *Privacy in Context*, Nissenbaum further develops her views on privacy as "contextual integrity". She uses a spatial metaphor pointing to the gap between the "heavens" of universal human principles and values and the "hard ground of concrete, gritty, detail" that contextual integrity is supposed to bridge.[255] "Contexts," she writes, "are structured social settings characterized by canonical activities, roles, relationships, power structures, norms (or rules), and internal values (goals, ends, purposes)".[256] Contexts are "essentially rooted in specific times and places" that reflect the norms and values of a given society.[257] Hence, for her, contexts are not *situations* that are constituted and constantly evolve and dissolve in experiential time-space.

---

243 Nissenbaum 1998, pp. 10ff.
244 Nissenbaum 1998, p. 37; van den Hoven 2001 p. 431.
245 Walzer 1983.
246 Nissenbaum 1998, p. 22.
247 Nissenbaum 1998, p. 30.
248 Nissenbaum 1998, p. 27.
249 Westin 1967/1960.
250 Gavison 1980.
251 van den Hoven 2001, p. 440.
252 van den Hoven 2001, p. 442.
253 Swanson 1992.
254 Bien 1985, p. 225.
255 Nissenbaum 2010, pp. 9f.
256 Nissenbaum 2010, p. 132.
257 Nissenbaum 2010, p. 134.

Nissenbaum's view of norms is basic for her approach of "contextual integrity". She adopts as a default position the view of norms as prescriptive, and not just descriptive, with regard to human action. She further distinguishes between "informational norms" as related to individual contexts from "context-related informational norms" as referring generally to the former. But this difference is not an opposition, since informational norms are "co-constitutive" of the second type.[258] Informational norms, including now both types, are common to senders, subjects and recipients of information that might be individuals and/or organizations, although she concentrates on single individuals. Not being restricted to defining information as belonging either to the private or the public sphere but to different contexts, Nissenbaum remarks that "attributes" or "information" types arise within an "indefinite array of possibilities".[259] This implies that privacy, for Nissenbaum, is not an attribute of a particular kind of information, but depends on the context in which it is shared, privacy being then a second-order attribute, to use the terminology of systems theory.

Contextual integrity as dealing with or presupposing given norms and principles, i. e. of what is usually called customs or ethos, could be considered as being essentially conservative or even subject to the "tyranny of the normal", particularly because norms and principles are supposed not only to be considered as descriptive but also as morally normative.[260] To avoid this, Nissenbaum writes that "a theoretical account of social contexts ought to leave room for the possibility that a society may, on occasion, revisit and scrutinize contexts and their respective values, potentially concluding they are unsound or unworthy".[261] She thus appeals for the critical function of ethical thinking on a given morality.

A critical appraisal of Nissenbaum's concept of privacy as contextual integrity from the perspective of whoness and a shared world approvingly acknowledges the change of perspective proposed by Nissenbaum with regard to the traditional dichotomy between the private and the public as well as to the view based thereon of the relation between an encapsulated and worldless 'I'-subject matched to private data. This is what we call the *what* in contrast to the *who* perspective. Nissenbaum crosses out this relation by calling attention to the underlying relation between individuals and their worldly life-contexts. Nevertheless, neither the question concerning the whoness nor the interplay between whoness and a common shared world is explicitly stated, let alone conceptually worked out. Instead, Nissenbaum's ethos-based view of privacy as "contextual integrity" rests on the presupposition of overarching and meta-contextual moral principles and values being pragmatically addressed from a contextual perspective. Eventually she has to acknowledge the limits of the contextual approach when facing the danger of tyranny arising from the predominance of one sphere and its values over the others, and look to the "heavens" of meta-contextual values and norms.

Nissenbaum's normative ethos-based contextual approach to privacy needs a deeper foundation in the experiential ethos of lived usages. But it is an important theoretical and pragmatic turn with regard to the traditional dichotomy between the private vs. public sphere no less than with regard to the concept of privacy as pertaining solely to personal data, which reduces the phenomenon of whoness to whatness. The question of trust is mostly seen on one side of the equation which means, in the case of the cyberworld, that it is located on the side of the owners and/or administrators of digital data about their 'subjects'. This paternalistic view of trust does not acknowledge the free and open interplay among selves in a shared world, but aims at substituting them in claiming that the cyberworld is the real world, where liberty now has its place rather than in any kind of individual privacy (which, in any case, is never an encapsulated, individualized privacy). This "knock-down" argument is paradoxically correct

258 Nissenbaum 2010, pp. 140f.
259 Nissenbaum 2010, p. 143.
260 Nissenbaum 2010, p. 160.
261 Nissenbaum 2010, p. 180.

if and only if liberty is now conceived as located within the (cyber-)world as digitally materialized by computer technology with its apparently unlimited possibilities of control that would assuage free agents about any unforeseeable future.

This homogenous, linear space-time axis of the cyberworld shines back onto the conception of liberty, by freeing it of its abyssal dimensions that can be bridged only by trust within reciprocal interchanges. This is the highest imaginable danger for privacy since it turns self and world into uniform tempo-spatial and computational dimensions in which the ethical difference between who and what eventually disappears. Selves existing in a world then become subjects matched with objective data-packets that can be mined in order to precalculate individual and collective behaviour. The issue of privacy in the context of the cyberworld precipitated by digital technologies then turns into a key ethical challenge for the self and the world in learning to resist the digital temptation, not by looking for metaphysical security in normative "heavens", nor by taking a "moral time out", but by unmasking digital globality as driven by individuals and/or organizations that pretend to put their 'liberties' beyond those of all other players on the basis of their power over mega-digital resources. Nissenbaum provides selves with some kind of guerrilla tactics so as not to lose sight of what is at stake when the digital Leviathan raises its head in specific contexts.

2.4.8 FLORIDI'S METAPHYSICS OF THE THREEFOLD-ENCAPSULATED SUBJECT IN A WORLD CONCEIVED AS INFOSPHERE[262]

The purported "informational nature of personal identity"

One probably must have spent a couple of years with Aristotle's *Metaphysics* to learn that traditional ontology is the investigation of "beings insofar as they are beings". Today, at the end of the scientific age, based tacitly on subjectivist metaphysics, the conception of ontology has shrivelled to the assertion, "The basic question of ontology is 'What exists?'"[263], where it is not asked what it means to "exist". Floridi does not represent any exception to this impoverished modern conception of ontology. In his article,[264] Floridi takes it upon himself "to explore the foundations of the construction of personal identities, by developing an informational analysis of the self. The broader thesis I shall defend is that ICTs are, among other things, egopoietic technologies or technologies of self construction, significantly affecting who we are, who we think we are, who we might become, and who we think we might become". The question concerning "who we are" is hence front and centre of Floridi's endeavours, although not as an existential-ontological question concerning whoness, but as a matter of "technologies of self construction" which, of course, presupposes that selves are constructed. This conception of constructed personal identity must then perforce serve Floridi when approaching, in particular, the phenomenon of privacy (see below). In this section, however, a deeper-lying critique of Floridi's informational metaphysics will be offered.

The problem Floridi sets up starting from "Plato's famous metaphor of the chariot" in *Phaedrus* is that of the unity of the self and how this unity is maintained "at different times and through changes," whereby linear time is assumed as self-evident.[265] The problem of unity of the soul, which Floridi equates with the self, is how a tripartite, "multi-agent system" (MAS) consisting of a charioteer, one good horse and one bad horse, can constitute a unity, as if this "tripartite analogy" could provide the basis for a well-grounded philosophy of the self. This analysis of the unity of a metaphorical soul is to constitute a contribution to a problem

262 This and all subsequent sections of this chapter are the final authorial responsibility of Michael Eldred.

263 Chalmers 2009.

264 Floridi 2012. Accessed August 2011 at http://www.philosophyofinformation.net/Articles.html Unless otherwise specified, all quotations in this section are from the PDF-file for this article. I will go through the article in what I hope is not all too excruciating detail.

265 Cf. by contrast Eldred 2009/2011, § 5.7.

of "egology", for which Plato's imagery for the soul is to be equated with the ego of the modern metaphysical subject, starting with Descartes, as if such a continuity could be assumed without further ado. "From Descartes onwards [...] the unity, identity, and continuity of the I, or self, as an entity become the subjects of an ontological investigation in their own right." This pretension to *ontology* is important in view of the merely *ontogenetic*, evolutionary *model* of self-constitution that, later in the article, Floridi will proceed to present without batting an eyelid. The question regarding "who we are" today is thus framed entirely within the modern metaphysics of the subject, and that in terms of third-person descriptions familiar already from Descartes, Leibniz, et al. that proceed from a self-evident understanding of the subject as a certain kind of 'what' rather than a 'who' (even when Descartes speaks of "I").

By slipping in a theory of multi-agent systems underneath as his foundation, Floridi is able to regard the soul or self or ego as a "complex, engineered artefact", again a kind of what that can even be engineered, thus continuing, indeed, the long history of productionist metaphysics launched by Plato and Aristotle, according to which beings qua beings are somehow produced, like a carpenter produces a table. This move of Floridi's invites a "shift from a phenomenological or descriptive approach to the self to a constructionist or design-oriented approach", a quotation that reveals Floridi's understanding of phenomology as mere ontic-factual description, as has become popular in the social sciences. That phenomenology could be the striving to bring what is most obvious and hence most hidden to light, namely, modes of being/presencing, does not occur to Floridi.

Following on from Plato, Floridi identifies two major problems in modern subjectivist metaphysics as "*diachronic* egology" which "concentrates on the problems arising from the *identification* of a self through time or possible worlds," and "*synchronic* egology," which "deals with the *individualisation* of a self in time or in a possible world", both being aspects of "an ontology of personal *identity*". Floridi concentrates in his article on the latter, making only brief comments on the former as a problem of how the self can be "modelled at a given level of abstraction" as a kind of "system" in which the main difficulty is to identify what is the same at different points of linear time. Such an ontology of the self is hence a theoretical construction supposed to "model" a certain "system", just like a scientist models reality with a theory on the basis of certain made-up hypotheses, interrogating reality with experiments to get the answers he needs to achieve an effective, successful intervention into this reality. The problematic of self and other, famously approached in Plato's dialectical thinking in both *The Sophist* and *Parmenides*, plays no role whatever in Floridi's considerations.

Floridi introduces the "narrative" subjectivist conception of the self's identity via a quote from Proust, according to which "we 'identify' (provide identities) to each other," via the representations in consciousness we have of each other by matching these representations with "the sound of his voice," etc. "We compose in our minds those ideas" (Floridi citing Proust), so that *identity* of a certain self is conceived as a compositum, a narrative, of representations in the consciousnesses of others (who are *different*). Floridi then proceeds to confuse this question of self-identity with that of individualization of the self, so that one must ask why he introduced the distinction in the first place.

Floridi then proceeds to claim that both approaches to the problem of individualization (or is it the problem of identification?) depend on "the right sort of informational skills" required to compose a unity of identity. So there is now a third approach to self-identity as informational unity, which is a problem that Floridi introduces with a long quote from Hume in which Hume proceeds from "all our particular perceptions", which Floridi glosses as "[bits or streams of information separate from each other]", and then becomes sceptically perplexed about *"the mind* [which] *never perceives*

any real connexion among distinct existences"". The dilemma for Hume is hence that the unity which is supposed to constitute "personal identity *arises* from consciousness; and consciousness is nothing but a reflected thought or perception", which Floridi glosses as "[information processing]". The problem for Hume is, apparently, that only sense perceptions are (posited to be) real, and reflected thoughts are (posited to be) unreal, merely ideal.

In Floridi's terms, the problem is how all the different bits of information, based on 'real' sense-perception information-gathering, floating around as representations in consciousness (one's own or those of others) are to be unified through some kind of information processing. Floridi then adduces Kant's solution for the unity of the information-processing subject that resides in the transcendental constitution of the subject in its unity prior to any experience of the world, i.e. prior to its information-gathering ways, but he is unsatisfied because Kant's transcendental argument (genuinely ontological within the constrictions of the metaphysics of subjectivity) does not explain ontogenetically "How such unity and coordination come to be there in the first place". Readers breathe a sigh of relief that finally they will be told a story.

Floridi's problem is that of the constitution of the *informational* self as an information-processing unity rather than a unity of disparate perceptions or narrative bits and pieces. He proceeds to solve it by abandoning any ontological pretensions whatsoever and replacing them by an account of how the "informational unity of the self may be achieved, or at least described, through a three-phase development of the self," clearly an ontogenetic-explanatory task that Floridi tackles by proposing a "model" whose "goal is ultimately that of explaining in what sense ICTs are egopoietic technologies".

Floridi then proceeds to present his "model" of the self as a three-stage encapsulation by a series of three "membranes" through which an individual is "detached" from its environment and becomes thus capable of "internal auto-organization". The three membranes are "the corporeal, the cognitive and the consciousness or simply 3C [which] seem to be the main stations at which the train of evolution has called". Such an ontogenetic, evolutionary story presupposes that ultimately the human being is a conscious subject encapsulated threefold within itself against the world.

With the second, cognitive membrane, "which allows the encapsulation of data for processing and communication," "intelligent animals" arise. Finally, "the third phase is represented by the evolution of the consciousness membrane. We move from pre-conscious (aware) to post-conscious (self-aware) systems once data become repurposable information, including conventional meanings (e.g. sounds become a national anthem)". In line with this hypothesized model, an a priori affinity with the unquestioned metaphysical presuppositions of AI research and neuroscience is plain. A statement such as "the consciousness membrane is softwired (programmable)" must be welcome to today's AI scientists, since it updates the metaphysical 'oldspeak' of a subject imbued with an intellect, and makes the problem of self-identity functionally operable.

The semantic membrane of consciousness in this narrative of the evolution of the I-self is brought into a connection with the ICTs that are said to be "the most powerful technologies to which selves have ever been exposed," leaving their mark on all three ontogenetically conceived membranes through "re-ontologisation". On all levels, the self is then *made* through technology, above all, through ICTs.

So, when Floridi comes to treat today's digital information and communication technologies that push the possibilities of writing as a memory aid into hitherto unimaginable areas, because all sorts of happenings in the world can be recorded through various digital media apart from mere writing, it is unwarranted to claim any *ontological* significance

for an *ontic-factual*, *historical occurrence*, to wit, "any technology, the primary goal of which is to manage records, is going to have an immense influence on how individuals develop and shape their own personal identities". The *temporal unity* of the self, at least toward the dimension of the past or been-ness (since it is not past and can be retrieved, whilst *simultaneously* being refused presence) is already tacitly presupposed by any claim for how today's digital ICTs enhance or detract from individual selves' technologically empowered possibilities to "develop and shape their own personal identities".

When Floridi remarks with regard to today's new digital ICTs, "the more memories we accumulate and externalise, the more narrative constraints we provide for the construction and development of personal identities," this may be true as an ontic-factual statement about our historical situation, but the observation itself presupposes ontologically that the self is already also, in an essential aspect, a shining-back from the world (cf. *2.2.2 Selfhood as an identification with reflections from the world*) in the sense of the narratives related about the self by others in the third person and the narratives each self tells itself in the first person about *who* it is.
Floridi's "model" of a unified self encapsulated in a threefold membrane turns out to be an imagination, a fantasy constructed in line with modern subjectivist metaphysics but contradicted by the phenomena themselves such as the digital gaze which contributes to the narrative and existential options out there with which the self may or may not identify. "The self tries to see how others see itself, by relying on information technologies, which greatly facilitate the gazing experience. The self uses the digital imaginary concerning itself to construct a virtual identity through which it seeks to grasp its own personal identity." Since digital data and the narrative related by them about somewho are as real as one can get in the digitized world, there is no occasion to speak of a merely "virtual identity" constituted by the digital gaze.

To identify even narratively, however, the self must be already out there with those narrative data, and not encapsulated within a consciousness membrane within whose sphere it constitutes itself as reflective self-consciousness which is thus conceived by Floridi's membrane model as the mirroring-back from the diaphanous consciousness bubble within which it is enclosed and captured. Rather, the self is always already ecstatically ex-sisting, i.e. out-standing, in the world, stretched out also temporally into three-dimensional time-space.

Floridi introduces in the final section of his article a concept from Aristotle's *Poetics*, namely, ἀνάγνωσις or 'recognition'. In Aristotle's thinking on tragedy, recognition is that phenomenon through which the character, such as Oedipus, tragically recognizes himself belatedly through the unfolding of events which, of course, in Floridi's informational metaphysics, amounts to a reinterpretation of one's third-person self-narrative on the basis of the receipt of new data packages from the infosphere.

Significantly, Floridi's adopted concept of recognition relates only to informational data packages telling a tale about the self's past. Even from the point-of-time after (A), the self is looking back in hindsight, not casting itself into future possibilities, although that is the point of Greek tragedy: the final downfall of the tragic character. What about the self's future? These data packages have not yet arrived, so how can they be taken into account? How can they be real for a realist model? This implies that the self has no future, because there exists no information from the future. Or, asked more cautiously, what is the ontological status, i.e. the mode of presencing, of futural "informational structures" (Floridi's preferred term for entities in his informational metaphysics of the infosphere)? Do they not yet exist? Do they exist only in fantasy, as the metaphysical tradition since Aristotle has supposed, or do they exist *as* futural scientific extrapolations of present scientific data?

Floridi views "the world as the totality of informational structures dynamically interacting with each other". In this infosphere-world, the ultimate informational structure is the threefold encapsulated self. "Selves are the ultimate negentropic technologies, through which information temporarily overcomes its own entropy, becomes conscious, and able to recount the story of its own emergence in terms of a progressive detachment from external reality." This says that selves are enclosed data packages that i) are made ontogenetically by a technology and ii) are a bulwark against informational entropy by concentrating and encapsulating information within itself, i.e. within the consciousness membrance, in such a way as to finally kindle the fire of self-consciousness. Of course, this narrative of the self is also just an imagined fantasy with which we can choose freely to identify or not.

Floridi's purportedly "ontological interpretation of informational privacy"

What Floridi presents as 'The ontological interpretation of informational privacy'[266] is in truth a merely sociological discussion for acronym fondlers of issues around informational privacy, undertaken with many historical comparisons of the capabilities of various "information and communication technologies", or ICTs. It is instructive to look more closely and concentratedly at what Floridi understands by ontology, "ontological friction" and "re-ontologization". Given the philosophical-ontological pretensions of the article's title, its largely sociological, historical contents, with moral over- and undertones and dilemmata, can be left to sociologists and historians and analytic moral philosophers. The question raised by the article's title is, properly speaking, What is informational privacy?, which breaks ínto two questions: What is information? and What is privacy? To such questions, the sociologist or analytical philosopher is content to provide definitional answers that mark the phenomenon in question off successfully and clearly from other phenomena. Such a procedure is altogether different from asking what these phenomena are as modes of being, i.e. as ways in which beings show up and present themselves in the world, e.g. *as* (bits of) information, or of the way in which privacy itself is to be understood as a mode of non-disclosive presencing of whos. Such questions have been addressed in previous chapters of this study (cf. esp. *2.2.4 The question concerning rights: personal privacy, trust and intimacy*). Here it is more a matter of looking briefly at what Floridi writes within the narrower umbra of these questions.

The aim of Floridi's article "is to argue in favour of a new ontological interpretation of informational privacy and of its moral value, on the basis of the conceptual frame provided by Information Ethics". He asks, "Why have digital ICTs made informational privacy one of the most obvious and pressing issues in computer ethics?" and asserts that new digital ICTs "have their roots in a radical and unprecedented transformation in the very nature (ontology) of the informational environment, of the informational agents embedded in it and of their interactions". Thus it becomes an issue to assess what Floridi understands by "ontology". As elsewhere, Floridi casts the world as the "model" of the "infosphere" as discussed in the preceding section. He introduces a central concept of his article: "'Ontological friction' refers here to the forces that oppose the information flow within (a region of) the infosphere, and hence (as a coefficient) to the amount of work required for a certain kind of agent to obtain information (also, but not only) about other agents in a given environment". An *ontic-factual* blockage to the flow of information, modelled on classical mechanics, is supposed to be elevated to the status of an "ontological friction".

Floridi then discusses whether "throughout history, informational privacy has constantly decreased in relation to the invention and spreading of ever more powerful ICTs," asserting that "this would be a simplistic and mistaken inference". He adduces, for instance, the phenomenon of anonymity that arose with large cities as a privacy-enhancing factor rather than a privacy-eroding one. This is

[266] Floridi 2006a. Unless otherwise specified, all quotations in this section are from the PDF-file for this article.

a sociologico-historical thesis having no ontological import, so it will be left to one side here. Floridi then proceeds to present digital ICTs themselves "as re-ontologizing technologies". What does this mean? Floridi breaks this down into five theses, but it can be said more succinctly as the digitization of information and its consequences. Since he casts the world itself as infosphere, for Floridi, the digitization of information amounts to a digitization of the world and, to an extent, its human inhabitants.

Secondly – and this point is basically Floridi's second thesis relating to "the homogenization of the processor and the processed" where he refers also to Turing – digital data (beings) can be automatically processed by executable code that is simply another digital string, i.e. a computing program. The Universal Turing Machine consists first of all of program code on the endless tape, followed by the digital data to be processed by the preceding program code. This does indeed amount to an ontological earthquake, because materially outsourced digital program code assumes a hitherto inconceivable autonomy vis-à-vis human beings in robots of all kinds that, supplied with electric power, *move on their own, steered by program code*, as if they were somehow alive.

After discussing various illustrations of friction in informational flow due to both old and new (digital) ICTs, Floridi turns to "assessing theories of privacy", of which he considers two: the "reductionist" (or consequentialist) and the "ownership-based" interpretations. The former focuses "on a variety of undesirable consequences that may be caused by its [information privacy's] breach", whereas the latter asserts that "a person is said to own his or her information" like other private property. Floridi points to inadequacies in these two theories and proposes instead his own so-called "ontological interpretation of informational privacy and its value" resulting from the advent in full force of digital ICTs. Informational privacy becomes "a fundamental and inalienable right" akin to the right to life and liberty. The person is thus not simply identified with its informational data as its other, but, for Floridi, simply is its informational data.

On this recasting, the human being becomes equated ontologically to an informational data package existing in the world cast *as* infosphere. "You are your information". However – *pace* Floridi – any identity presupposes and preserves difference, and vice versa. In this instance, it is the living, breathing human being, existing as an open temporal clearing for the presencing and absencing of beings in the world that identifies with possible castings for its own existence as mirrored back from the world, which is always more than mere 'information'.

All subsequent discussion by Floridi of the consequences of equating (rather than identifying) a person with his or her digital information is therefore otiose, for it is based on a skew-whiff ontological conception of the person.

2.4.9 ON CHARLES ESS' APPRAISAL OF FLORIDI'S INFORMATION ETHICS

Ess' 2009 article sets out "to evaluate Floridi's philosophy of information (PI) and correlative information ethics (IE) as potential frameworks for a *global* information and computing ethics (ICE)". He claims for Floridi, "Indeed, subsequent history may judge that his PI and IE stand among a handful of prominent developments of the first six decades of Western ICE (if we begin with Norbert Wiener, 1948)." Here I will concentrate on the foundations of Floridi's theories, viz. "PI as an ontology" which Ess, in the fourth section of his article, cursorily puts into relation to "the Heideggerian components of Rafael Capurro's intercultural information ethics". Ess' appraisal of "Floridi's treatment of privacy and the closely related matter of what counts as personal data" also deserves attention here. Ess is particularly interested in extending and making more robust Floridi's PI and IE in a *global* context by moving in the direction of a "new,

post-Cartesian conception of the self and ethical imperatives" that makes it possible to encompass non-Western thinking such as Buddhism and Confucianism. Does Floridi's ontology really represent a move beyond Cartesianism? Preceding sections have already shown that it does not, but let us examine Ess' presentation.

Informational ontology

As Ess cites, Floridi opens his ontology by postulating "'to be is to be an informational entity' (Floridi, 2008 p. 199)." which, Ess claims, is a "radical turn". Given Floridi's commitment to subjectivist metaphysics (cf. *2.4.8 Floridi's metaphysics of the threefold-encapsulated subject in a world conceived as infosphere*), this is questionable. With regard to Floridi's basic, all-encompassing, ontological postulate, the question is immediately posed: Does Floridi clarify the very meaning of being? No. And neither does Ess. Furthermore, the very term 'information' is drenched in the Western metaphysical tradition, as shown in detail by Capurro, starting with Aristotle's μορφή. and Plato's εἶδος, standardly rendered in English precisely as 'form'. In Ess' eyes, taking information as a foundational ontological category is supposed to enable an encompassing of ethical traditions beyond a merely Western horizon by shifting from the emphasis on the "(human) moral agent as primarily a 'psychic atom'—i.e., the *individual*". Information as non-human seems to provide an alternative to Western 'humanism'. But who is it, if not the human being, who is or could be open to beings *as* beings, including to beings *as* information?

Furthermore "*individual*" is no innocent term, being not tied solely to the Cartesian subject of mathematized knowledge, since it is associated primarily with the modern individual who has only become historically possible in the last four hundred years through the coming to hegemony of a *reified* mode of sociating commonly, but misleadingly, referred to as 'capitalism based on private property' (cf. *2.2.6 The private individual and private property as a mode of reified sociation: the gainful game (classical political economy, Marx)*). Modern political philosophy to the present day continues in misconceiving the individual as an "atom", whereas in truth, the individual is itself a relatively late historical mode of *dissociated* human beings *associating* with one another through the mediation of privately owned things. This modern individual is the socio-political counterpart to the modern, encapsulated, conscious subject whose blue-print was first drafted by Descartes. As shown in preceding sections, Floridi is still captive to the metaphysics of the encapsulated subject.

Ess discusses next an *ethical* implication of Floridi's informational ontology, namely, that it postulates "reality qua information as intrinsically valuable". This, Ess claims, enables Floridi to overcome a "modernist emphasis on the distinction between *things* and *value*" that arises from the Cartesian dualism between the conscious subject (which, purportedly, alone is valuable) and material things that are surrendered to mastery and exploitation by the modern subject. Ess overlooks thereby that the discourse on the value of things themselves has also a long history in modern political and moral philosophy that gave rise to political economy and economics.

Such valuableness of things can extend to the appreciation of the *natural environment* itself as valuable for human dwelling on the Earth when human beings themselves, as they are doing today, come to an appreciation of the destructiveness of human productive activities for the environment on a global scale. It is only humans who historically can learn to care for and thus value the environment. Things, including Floridi's informational entities, are not "intrinsically" valuable, but only within a world inhabited by human beings. If we humans weren't here, there would be no question regarding value at all.

That informational entities are (postulated as) intrinsically valuable leads on to Floridi's postulation of the "flourishing" of all entities *as* information. Ess defends this notion of flourishing by citing Floridi's "insistence on the goodness

of being" with its Augustinian resonances. Since, in Floridi's ontology, all entities show themselves *as* information, this amounts to an informational casting of the being of beings in toto, whilst leaving the question as to the meaning of being itself unasked.

For Floridi, the opposite of flourishing is "entropy", which "is increased when Being, interpreted informationally, is annihilated or degraded."[267]. This mention of "Being" confuses being itself with beings *as* beings, since Floridi's ontology only cast all *beings* as information.

Informational privacy

When Ess turns to evaluating what Floridi's informational ontology and its associated ethics of informational flourishing and annihilation have to do with informational ethics and privacy, it is noticeable that, under the impact of Tavani's critical assessment of Floridi's theory of informational privacy (cf. previous sections), Floridi indulges in some backpeddling. He writes in response to Tavani, "informational ontology may help us to understand an individual as constituted by her information [and] is meant to contribute and be complementary to other approaches to e.g. physical or mental/psychological privacy". In view of the ontological postulate, "to be is to be an informational entity", this amounts to a big climb-down. Floridi's ontology becomes a mere framework model complementary to, and *alongside* other models, thus admitting a pluralism of approaches.

The consequence is a theoretical arbitrariness and disorientation consonant with an incoherent pluralism in which the issues that call for clarification are set adrift on an apparently tranquil sea of toleration for mutually incompatible approaches to the same phenomena. Fundamental ontological questions are left unasked and, above all, it is not seen that Floridi's informational ontology is a specific historical casting of the being of beings that is unaware of its captiveness to the long Western metaphysical tradition of successive metaphysical castings of the being of beings.

Ess does not see things this way at all, but instead, in his concluding section, praises Floridi for providing, on the basis of his "'lite' form of information ontology" an information ethics that is "one minimalist framework among others". But how can a basic casting of entities as informational be pluralistic?

Getting over the subject-object split

Ess also praises Floridi for being "among a growing array of philosophers enjoining us to move beyond the Cartesian mind–body split", but overlooks that Floridi's ontology of the encapsulated subject of consciousness (see preceding sections) does not overcome the Cartesian subject–object split, which is more fundamental. In fact, since in Cartesian subject–object dualism, it is precisely the bodily senses that mediate between the subject and the world of objects, it is questionable whether a "mind–body split" in Cartesian metaphysics is the crucial issue at all, but rather the Cartesian dualism between res cogito and res extensa. Ess confuses what today is meant by cognition as the activity of thinking with the breadth of the Cartesian cogito, which encompasses all that is represented in consciousness, including feelings. So Ess' plea for taking notice of embodied feelings and proceeding beyond "a purely Cartesian emphasis on the self qua disembodied mind" in a "move closer to both pre-modern Western and non-Western conceptions" is a misconception. The Cartesian mind already *is* embodied and *has* feelings.

The problem is rather that in all subjectivist metaphysics, including Floridi's, feelings are encapsulated within the embodied subject rather than being moods out there in the world to which human beings find themselves attuned (in German: sich befinden in einer Befindlichkeit), and *can* find themselves attuned, because human being itself is an ecstatic, ex-sistential (literally out-standing), quivering openness to the world (and not just to objects in the world).

267 Floridi 2008, p. 200.

2.4.10 BEAVERS' RESPONSE TO AN OBJECTION BY FLORIDI TO AI BY REVERTING TO HUSSERLIAN SUBJECTIVIST PHENOMENOLOGY

Beavers (2002) takes up an objection by Floridi that "because computers, or computer programs, are locked in microworlds and human beings are not, AI research cannot approximate human intelligence, which is open-ended and able to deal with a broad range of contingencies."[268] which he proposes to overcome by showing the appropriateness precisely of microworld phenomenlogies. Beavers starts by restricting legitimate, pertinent phenomenology to the Husserlian kind, to the exclusion of both Hegelian and Heideggerian phenomenology. Kant gains a place beside Husserl because both think within the problematic of the constitution of objectivity from within subjectivity. He wants to keep things encapsulated within a subject's consciousness to keep things amenable to cognitive science and AI. From the outset the focus is on *causal explanation* and *effectiveness* in line with the demands of "science", "cognitive science" in this case.

"Let us define as 'ontological enveloping' the process of adapting the environment to the agent in order to enhance the latter's capacities of interaction."[269] This "ontological enveloping" in Floridi's sense is merely ontic-factual adaptation to the features of a restricted segment of the world. In Floridi's own words, it is "the process of adapting the environment to the agent in order to enhance the latter's capacities of interactions", in other words, the refinement of a model.

Beavers puts his finger on the weakness in Floridi's schematic-subjectivist ontology by pointing to the superiority of Kant's and Husserl's ontologies of subjective world-constitution, although in doing so, he truncates Kant to mirroring "the fundamental laws of science", thus keeping things 'under control' for the sake of control. Floridi's critique of AI "that human experience is open-ended and therefore not reducible to a microworld" overlooks the fundamental, genuinely ontological point (within the limits of Kantian and Husserlian subjectivist ontology) that computers do not and cannot constitute within their processors even a microworld.

Beavers fails to see this, thus levelling human being with computer being. Instead he focuses on the possibility of the (ultimately practical) usefulness of a Kantian/Husserlian microworld phenomenology.

The phenomenological fallacy here is that it is assumed (empiricistically, thus misunder-standing both Kant and Husserl) that only sense data are given to consciousness, and that these sense data are processed into the representation of an object. But what is given to the mind by the world is not merely a constant flow of sense data, but the world itself and the beings in it that present themselves, first of all, AS SOMETHING. The category of something must be understood and taken for granted a priori to even see anything out there in the world and take in sense data about it. However, for subjectivist metaphysics, that something is out there in the world is, in turn, an a priori (transcendental in the Kantian sense, i.e. prior to experience) projection from the mind that constructs within itself some such thing as an object – the objects out there in the world AS objects are projections of subjective consciousness. The "phenomenological representation [within consciousness ME] is the extra-mental world *as we take it to be*." The world does not present itself to us, but rather, *as we take it to be*. Hence, strictly speaking, objects exist only within subjective consciousness, and any objects out there in the world are only the projections of imagination.

Through his line of thinking, Beavers paints himself into the corner of the realist/idealist dilemma: Is the world really out there? To rely on Kant is to adopt a subjective idealism, but Beavers must try to elude this fate. This requires a leap of faith: "For it could well be the case that the

268 Beavers 2002 with reference to Floridi 1999.
269 Floridi 1999, p. 214.

phenomenological world, the transcendence in immanence constituted out of sense data by mental processes, maps adequately onto the world of things in themselves. Just maybe we get things right."

The subject/object split is essential for the applicability, in any form, of phenomenology to cognitive science and AI in order to have an encapsulated, constructible starting-point whence to interact with things in a restricted microworld. If the human mind were not thus encapsulated, but rather always already out there in the world among beings of all kinds,[270] there would be no toehold for cognitive science to make itself useful. Against the phenomenological evidence, cognition is posited 'realistically' and 'materialistically' to take place in "processes [that] are instantiated in the brain" locatable and enveloped within the body, and these brain processes then can be modelled and programmed as digital algorithms processed in a digital processor. Thus, American pragmatism aims to cut through the turgid prose of Husserl and German subjective idealism to wrench out what is useful to realist, materialist, cognitive science. Insofar, what Beavers offers is only a slightly more sophisticated subjectivist ontology than Floridi's crude, schematic one (see preceding sections).[271]

2.5 INTERCULTURAL ASPECTS OF DIGITALLY MEDIATED WHONESS, PRIVACY AND FREEDOM

Rafael Capurro

2.5.1 PRIVACY AND PUBLICNESS FROM AN INTERCULTURAL VIEWPOINT

Recent research in information ethics shows that the notion and practices of privacy vary in different cultural traditions, thus having an impact also on digitally mediated whoness and freedom.[272] This intercultural discussion is still in its initial stages with regard to the 'Far East'[273] and also African and Latin American cultures, just as it is in comparative studies between, for instance, Europe and the United States as addressed, for instance, by Helen Nissenbaum (cf. *2.4.7 An appraisal of Nissenbaum's Privacy in Context*) and Beate Rössler (cf. *2.2.10 Privacy as protection of individual autonomy – On Rössler's The Value of Privacy*). How and as whom we reveal and conceal ourselves and our selves is not just an abstract conceptual matter, but is always concretized and rooted in cultural traditions. What is common and what is different shines forth from different perspectives

270 Cf. Eldred 2012.

271 Addendum by Rafael Capurro: Beavers thinks that phenomenology has to do with the first-person perspective and science with the third-person perspective. In this he is both right and wrong. He is right insofar as the phenomenologist tries to gather (λέγειν) and express what shows itself to him as 'his own'. But he is wrong insofar as he believes that that amounts to mere descriptive subjectivism or esoteric Wesensschau (contemplation of the ideas) from within a subject, since I put that which I take in and perceive (or more precisely: what I perceive already together with others) at their disposal and ask: Do you see that the same way as I do? The phenomenological contemplation of essence is anything but esoteric because it wants to express, as precisely as possible, what the (exoteric) phenomena show of themselves, apart from preconceptions or any kind of interposed theoretical schema or model. A table is a table, and not primarily a heap of physical data that I take in through sense organs and 'process' into the representation of a table in my consciousness. And a table is never merely just a table, but always already woven into an interconnection with other things, together with which the table has its determination *as* being-good-for this or that and so 'is' in the world. Of course, such determinations are not eternal, and they change in their ontic-factual detail, but within a world things are simply what they are. With regard to the modern scientific standpoint of objectivity, this standpoint cannot be separated from the 'subjective' standpoint in the sense just adumbrated, since science, too, is done by individual human beings. However, in this scientific context, the 'intersubjective' examination is subjected to other methodological yardsticks and boundary conditions, especially of a quantitative kind, which also are not eternal. Otherwise, we could never have any scientific revolutions that fundamentally change the paradigm. Beavers neglects these aspects, among others, and instead speaks of a schematic subject/object split that from the outset falsifies the phenomena at hand that are of concern, thus falsifying also phenomenology and science, and that leads nowhere except, perhaps, to a manipulation of the world through computers programmed with so-called AI.

272 Ess 2010; Capurro 2008; Ess 2008; Brey 2007; Capurro et al. 2007; Hongladarom & Ess 2007; Ess 2006; Ess 2005.

273 The term 'Far East' goes back to European colonial history. The French sinologist and philosopher, François Jullien, has proposed the symmetrical code "Far East – Far West" ("Extrême Orient – Extrême Occident") to make clear the one-sided European perspective (Jullien 1995, 2008).

that in some cases appear to be incompatible, although not necessarily contradictory. But even in these cases, as we shall see in the following analyses, various options for common practices and regulations are possible. The emphasis on the latter should not overlook, however, the deeper cultural layers as well as the foundational narratives on privacy and publicness.

We are still far from a global digital culture of mutual respect, validation and appreciation based on trust with regard to such cultural differences. Trust is engendered by an understanding of the otherness of the other(s) self/selves, enabling new forms of interplay between personal and socio-cultural whoness and opening new spaces of freedom to show ourselves and our selves off and also withdraw from such self-display in both the cyberworld and the physical world.

The following overview of implicit and/or explicit notions of privacy, particularly in the cyberworld context, in the Far East, Africa and Latin America, is a first attempt limited not only in the choice of cultures but also in the treatment of their inner complexity. There is no intent to simplify by using geographical markers. The few examples of differing narratives on privacy and publicness should be understood as illustrations of different ways of living the intertwining of personal and socio-cultural whoness according to changing rules of play for concealing and revealing who we are, mirroring our selves in and to each other. My self is always my self with other selves in a shared world.

We start with what can be regarded as a privative mode of whoness, namely the 'denial of self' in Buddhist and community-oriented cultures. In a second step, mostly implicit views on publicness and privacy in Latin America will be discussed, whose numerous and rich indigenous cultures, along with various forms of hybridization with European modernity, in particular in the way privacy in the cyberworld is played out, remain still largely a matter for future analysis. Finally, we take a look at African traditions, particularly the concept of *ubuntu*.

2.5.2 THE FAR EAST

Japan

In their seminal paper 'Japanese conceptions of privacy: An intercultural perspective', Nakada and Tamura write, "Japan is a complicated country – even for Japanese people themselves. Indeed, their lives are full of contradictory matters, including the problems related to privacy. People want to be free and pay attention to a 'right to control one's personal information,' but at the same time they want to get 'true' friends by sharing their secret information concerning their private, personal experience."[274] This can be said, of course, of any culture, but what is paramount is to analyze such "complicated matters" that shape lives in their uniqueness and, in particular, to see how selves understand themselves through digitally mediated whoness.

Before addressing the key issue of 'denial of self' (*Musi*), Nakada and Tamura analyze the framework that enables a proper understanding of the Japanese self or "Japanese minds", and of the view of privacy and publicness from this Japanese perspective. They start by explaining "a dichotomy between *Seken* and *Shakai* in Japanese minds."[275] *Shakai* means the principles and values adopted from the 'Far West', i.e. from Western modernity, while *Seken* means the traditional Japanese customs as shaped by Shinto, Buddhism and Confucianism. At the same time, they point to another layer of "Japanese minds", namely *Ikai* which is "the aspect of the world from which evils, disasters, crimes, and impurity" emerge,[276] where '*i*' means different and '*kai*' means world. But *Ikai* means also "the world in which people can find certain kinds of hidden mental bodily energy as well as freedom".[277]

274 Nakada & Tamura 2005, p. 27. See also Nakada 2007; Nakada & Capurro 2009; Mizutani et al. 2004.
275 Nakada & Tamura 2005, p. 27.
276 Nakada & Tamura 2005, p. 27.
277 Nakada & Tamura 2005, p. 29.

Taking as an example a homicide, they show how private details about the victim's family were reported in the newspapers that contradict partly Western or *Shakai* standards of privacy protection, while a survey among students showed that they approved of publishing such news because it can help to find out the 'truth' of the matter and "share certain aspects of the meaning of this tragedy."[278] Nakada and Tamura interpret the students' reaction as coming from *Seken* and *Ikai*. If this interpretation of "Japanese minds" (which amounts to the specifically Japanese way of being-in-the-world) is correct, then it can be inferred that Japanese selves and world are shaped by the trichotomy of *Seken*, *Shakai* and *Ikai*. Another important aspect of Japanese being-in-the-world concerns the notions of *Aida* or 'in-between' and *Musi* or 'denial of self' as analyzed, for instance, by the Japanese psychiatrist and scholar, Bin Kimura.[279] They explain the relation between the two notions as follows: "In an objective way, 'between' or 'in-between' is nothing, but for dwellers of *Seken* or *Ikai*, 'between' or *Mu* is an ontological way to get to the sources of hidden power or 'true' subjectivity. In addition, 'between' seems to be related to certain types of shared or intersubjective meanings, especially 'common senses' – including the range of normal or expected behaviours in Japanese culture and settings."[280] Although this explanation is based partly on and biased by Western notions of subjectivity, it clearly points to what constitutes the Japanese self, namely, the negation of such a notion of an isolated and worldless subjectivity or, in Japanese terms, of a self addressing herself as divorced from *Aida* or 'in-between', i.e. from the openness of a shared world. They write, "*Mu* means 'nothing' or 'denial' and *si* means 'self' or 'subjectivity'. So *Musi* means 'denial of (surface) subjectivity'. In our culture it is often said that *Musi*, denial of subjectivity, is the best – but 'hidden' and difficult – way to learn fine arts, martial arts and so on."[281]

From the perspective of whoness, *Musi* amounts to questioning the Western standard view of subjectivity, whose autonomy is supposed to be protected by privacy. At the same time, the trichotomy of *Seken*, *Shakai* and *Ikai* as which "Japanese minds" shape their selves in their interplay with the world makes apparent the problem with the Western notion of privacy, namely, that it is limited to *Shakai*. The authors write, "But one thing is clear: privacy is not something like an 'intrinsic good' – to use a term by Deborah Johnson – for us. For example, expressing or sharing (parts of) one's privacy seems to be a popular and traditional way to get good personal friends in Japan."[282] Following the Buddhist tradition of "self-purification" developed by Shinran in the Kamakura era (1192-1333), giving up one's 'private minds' "is to view oneself from the point of view of Buddha."[283]

The difference between notions of privacy in the 'Far West' and the culturally fashioned Japanese way of being who in the world is further developed with regard to the notions of *Ohyake* and *Watakusi*, which are the standard translations of 'public' and 'private'. *Ohyake* means originally 'big house' and refers to the imperial court and government, whereas *Watakusi* or 'not *Ohyake*' means "partial, secret and selfish".[284] *Watakusi* is related to *Musi* or 'denial of self', *si* in both cases meaning 'I' or 'private' or 'oneself' with negative connotations, as already noted.

For the Western notion of privacy a borrowed word, namely *puraibashii*, was created as a legal term in 1964 and opposed to *Ohyake* but having a different meaning from that related

278 Nakada & Tamura 2005, p. 28.
279 Kimura 1972.
280 Nakada & Tamura 2005, p. 29.
281 Nakada & Tamura 2005, p. 29.
282 Nakada & Tamura 2005, p. 30.
283 Nakada & Tamura 2005, p. 30.
284 Nakada & Tamura 2005, p. 32.

to *Watakusi*. This shows once again the complexity of "Japanese minds", i.e. the ways in which Japanese exist as who in their world. Nakada and Tamura write, "We have a hypothesis that there are in fact two 'axes' defining 'public' and 'private' issues currently in Japan. One is the 'public' and 'private' axis (i.e. as anchored in the loan word *puraibashii*) and the other is the *Ohyake / Watakusi* axis. They are intermixed."[285] On the new axis, privacy as *puraibashii* meant the right to disallow interference from others and changed its meaning, after the development of information technology, to 'the right to control one's personal information'. But, in contrast to the Western concept of privacy, in Japan "privacy is discussed as a 'crisis of privacy issue' and not as the basis for democratic concern as it has been discussed in Western information ethics. In this way, Japanese society may have introduced one aspect of the concept of privacy as used in the West – but not the whole of it."[286] Hence, for the Japanese self living on the *Ohyake / Watakushi* axis, there is no privacy problem related to, for instance, open web diaries, where Japanese can conceal and disclose their selves in differently from how they do face-to-face in their daily lives that are ruled by *Seken* or its synonymous *Ukiyo*, meaning 'this transitory world'. "This means", the authors conclude, "that if communication on the Internet is nothing but another version of *Watakusi*-activity for the majority of Internet users in Japan, the Internet is at least partly a continuation of *Seken* (*Ukiyo*) event at this present time. And in fact, this continuation has been confirmed in our research in a number of ways."[287]

Thailand[288]

Soraj Hongladarom and other Thai ethicists have discussed privacy issues particularly in the context of the introduction of a national digital personal identity card in a country with no specific law protecting personal information.[289] The threat of political abuse raises the issue of the nature of privacy and its justification. Hongladarom explores this question from the perspective of two famous Buddhist sages, namely Nagarjuna (c. 150-250 AD), founder of the Mahahayana Buddhism, and Nagasena (c. 150 BC). He writes, "The reason I believe the Buddhist perspective is important in this area is that Buddhism has a very interesting claim to make about the self and the individual on whose concept the whole idea of privacy depends."[290]

In Hongladarom's view, the fact that Buddhism rejects the individual self does not mean that it rejects privacy. To elucidate this counter-intuitive argument, Hongladarom distinguishes between the absolute and conventional level of assertion. From an absolute standpoint, there is no distinction between subject and object. If there is no inherently existing self, then privacy is grounded in the conventional idea that it is necessary for democracy, which means that privacy has an instrumental status rather than being an intrinsic or core value.

Privacy as practised in everyday life is not denied in Buddhism. It is in fact justified as an instrument for the end of living harmoniously in line with democratic ideals. But "from the ultimate perspective of a Buddha, privacy just makes no sense whatsoever."[291] Violations of privacy are based on the three "mental defilements" (*kleshas*), namely greed, anger and delusion, the antidote being to cultivate love and compassion. He writes, "Compassion naturally arises from this realization when one realizes that other beings are no different from oneself. All want to get rid of suffering, and all want happiness. The benefit of this realization for information ethics is that compassion is the key that determines the value of an action."[292] Compassion is the

285 Nakada & Tamura 2005, p. 33.
286 Nakada & Tamura 2005, p. 33.
287 Nakada & Tamura 2005, p. 34.
288 The following analysis reproduces the findings in Capurro 2008 pp. 654-656.
289 Hongladarom 2007; Ramasota 2007; Kitiyadisai 2005.
290 Hongladarom 2007, p. 109.
291 Hongladarom 2007, p. 120.
292 Hongladarom 2007, p. 120.

basic mood of Buddhist experience of the uniqueness of the world and our existence that we have to care for.

China

The Chinese ethicist, Lü Yao-Huai, writes, "In the Chinese cultural tradition, ethicists pay special attention to the concept of 'Shen Du'. [...] 'Shen Du' means that 'a superior man' must be watchful over himself when he is alone."[293] He illustrates this with the following quote from *The Great Learning*, one of the *Four Books* of Chinese classic texts selected by the neo-Confucian scholar, Zhu Xi (1130-1200): "There is no evil to which the mean man, dwelling retired, will not proceed, but when he sees a superior man, he instantly tries to disguise himself, concealing his evil, and displaying what is good. The other beholds him, as if he saw his heart and veins; – of what use is his disguise? This is an instance of the saying – 'What truly is within will be manifested without'. Therefore, the superior man must be watchful over himself when he is alone."[294] According to Lü, *Shen Du* is a key notion when dealing with the question of the self, particularly within the context of the cyberworld, since it addresses the question of reducing "proactively [...] the number of online activities that violate legal frameworks."[295] Lü focuses on the self in his relations to himself and to others – the masculine might be a bias in Zhu Xi and, indirectly, also in Lü – based on the possibility of concealing and revealing who they are as selves. He critically addresses this issue with regard to the predominance of English on the internet in a paper presented to the first international symposium on intercultural information ethics held in Karlsruhe, Germany in 2004.[296] He writes, "The preferred scenario is, of course, multi-directional intercultural dialogues and channels. [...] in order to avoid being assimilated by English, the non-English-speaking people, especially in developing countries, must preserve the cultural characteristics of their homelands when they develop information technologies and information societies. [...] The local cultures of their homelands are the actual intellectual content embodied in the right to communicate for people from different countries."[297] Although in the meantime things have changed with regard to the predominance of English on the internet, the issue of whoness addressed from a Confucian perspective remains as crucial as it was in 2004.

Lü criticizes the historical analyses of the Chinese notion of privacy by McDougall and Hansson[298] as referring "primarily to studies of Chinese elites, focusing on the gentry and/or rulers" instead of giving an account of today's views on privacy, particularly among ordinary people. Lü maintains there is an ongoing transformation of contemporary Chinese "consciousness" of privacy – which means a transformation of the Chinese self – starting with economic and political reforms since 1980.[299] This change comprises three main aspects:

1. "[...] individuals gradually expand their self-consciousness of a right to privacy. Earlier, Chinese in conversation, especially between friends, would usually feel free to talk about anything (with the exception of some sensitive political topic). But now, if someone's question to a conversation partner deals with matters that the partner does not want to make public – the conversation partner usually declines to answer the question, on the plea that 'this is my privacy'.[300]

293 Lü 2007, p. 70.
294 Lü 2007, pp. 70-71. Quote from *The Chinese/English Four Books* Legge et al. 1992 p. 9.
295 Lü 2007, p. 71.
296 The symposium Localizing the Internet. Ethical Issues in Intercultural Perspective was sponsored by the Volkswagen Foundation (see http://icie.zkm.de/congress2004). The proceedings were published in Capurro et al. 2007. On 28-29 October 2010 the International Conference on China Information Ethics was held at Renmin University in Beijing. Issues of privacy and data protection were discussed in group meetings based on short presentations. See http://www.capurro.de/home-cn.html
297 Lü 2007, p. 73.
298 McDougall & Hansson 2002.
299 Lü 2005, p. 7.
300 Lü 2005, p. 8.

2. "[...] many Chinese today are no longer inclined to interfere with what they perceive to be the privacy of others: indeed, to some extent, they now show respect for others' privacy."[301]

3. The common Chinese concept of privacy *Yinsi* ('shameful secret') has been expanded to include "all personal information (i.e. whether shameful or not) that people do not want others to know."[302]

With the rise of the internet in the 1990s, the question of data privacy emerged in China. In his review of three recent (2003-2004) Chinese articles on privacy, Lü points to the influence of Western individual-oriented thinking on privacy with regard to respect and informed consent, while at the same time the right to privacy from a traditional Chinese perspective is conceived as being based on social requirements (security of society, stability of the social order).

A basic issue common to Far East cultures involves the practice of indirect speech, i.e. of the self concealing and *at the same time* revealing herself through language or, more precisely, through silence.[303] The Daoist tradition developed a *dao*-centred self, indirect speech being the adequate way to be part of a permanent process of becoming since it leaves open future possibilities of being. According to Chuang Tzu (370-301 BC), self-awareness consists in learning to breathe as a medium between the world, the '*dao*' and the self.[304]

2.5.3 LATIN AMERICA

Latin American cultures came about through the violent encounter between indigenous traditions and nascent European modernity. Indigenous collectivism faced premodern, particularly scholastic thinking, that praised the individual as a person no less than liberal traditions do, which are based on the idea(l)s of work, private property, competition and technology.[305] As the Argentinean philosopher, Rodolfo Kusch, writes, "The ways of life of the Indian and the well-off city dweller are impermeable to each other. On the one hand, the Indian retains the structure of an ancient form of thinking, a thousand years old, and on the other, the city dweller renews his way of thinking every ten years."[306] This "ancient form of thinking can be grasped with regard to the concept of 'reciprocity'. Indigenous people were not properly remunerated for their work, "because everything was taken by the cacique (or *mallkus*) [...] the indigenous worker is only repaid with food."[307] The equivalent of "reciprocity" in Aymara is *ayni*, "which means 'the one obligated to work for another who worked for him.'."[308] If the indigenous worker was obliged to give everything he produced to the Inca, but not to the Spaniards, there was nevertheless a reciprocity from the side of the Inca, namely the obligation "to refrain from interfering with the stockroom of the domestic sphere."[309] This dichotomy between the public and the private sphere in Inca culture has a parallel in the Greek dichotomy between *agora* and *oikos*. The 'domestic sphere' of the Inca worker was no less important for his self that the obligation to give his powers and the products of his work to the

301 Lü 2005, p. 8.
302 Lü 2005, p. 8.
303 Capurro 2010/2011.
304 See Jullien 2005, pp. 71-75.
305 See von Barloewen 1992, p. 132. On Latin American cultures from a philosophical perspective see Kusch 1962 and 2010. There are several studies on the history of private life in Latin American countries such as Argentina (Cicerchia 1998; Devoto and Madero 1999), Brazil (Novais and Moritz Schwarcz 1998), Chile (Sagredo and Gazmuri 2005) México (Gonzalbo 2004) and Uruguay (Barrán et al.1996).
306 Kusch 2010, p. 2.
307 Kusch 2010, p. 91.
308 Kusch 2010, pp. 92-93.
309 Kusch 2010, p. 93.

mallku, or chief. The system underlying this 'reciprocity' was not contractual, but based on the *pacha* or mother earth as something prior to the separation of a 'subject' from an 'outside, objectified' world. Kusch writes, "*Pacha*, instead, refers to a concept more properly related to what we call a subject, and it is located in a terrain prior to that of the perception of things. Here we have a subjectified, private space and time that refers to a vital habitat where *our* time and *our* space melt into the pure fact of living here and now when this involves the time of *my* life, *my* family, and in this place, the place of *my* community. All of this implies naturally an indiscriminate vision of external reality."[310] Although Kusch is employing the modern European notion of subject, he describes the phenomenon of self of the indigenous Inca which implies not only an original plurality of selves building a community, but also an original relation of the community to nature.

The Latin American 'who' is just as much an indigenous person as an urban inhabitant. Kusch writes, "If the urban dweller were to ask himself at this point, 'Who am I?', he would see himself reduced to a 'just living,' carrying his absolute on his back and a *who* that is lost in mystery. This nebulous *who* is the sum of what one achieves through this path. But it is a lot."[311] At this point, Kusch's analysis of Latin American indigenous whoness intersects with the Buddhist experience of the simple 'being there' ("estar ahí") of a person.[312]

The debate over intercultural information ethics in Latin America has only just begun.[313] There is a lack of philosophical and empirical ethical analysis on privacy,[314] particularly from an intercultural perspective and in relation to the internet.[315] One of the pioneers in the field of information ethics in Latin America is Daniel Pimienta, who created the virtual community MISTICA that produced in 2002 the document 'Working the Internet with a Social Vision'.[316] Point 5 of Section 13 poses the following questions with regard to "the defense of protected spaces on the Internet and the dissemination" of local knowledge:

"a. How do the actions that are promoted boost the production of local contents?
b. What level of participation do the people with whom we work have in the development of local contents?
c. To what extent do actions which are promoted allow to disseminate and promote local contents?
d. In what way is the Internet promoted as a space of expression for the less favored and for popular cultures?"

310 Kusch 2010, p. 94.
311 Kusch 2010, p. 171.
312 Kusch analyzes the difference between the Spanish verbs for 'to be', namely 'ser' and 'estar'. "[...] 'estar' comes from the Latin *stare*, 'to stand up', which implies restlessness, *Ser*, on the other hand, comes from *sedere*, 'to be sitting down, which connotes a foundation from which springs the possibility of definition'." (Kusch 2010, p. 160), 'Estar' is closely related to the indigenous *pacha*, the experience of 'just living', Latin America being a culture of 'estar'.
313 The first paper on intercultural information ethics from a Brazilian perspective is probably that by Dürmaier 2008. See Capurro 2009. The first Brazilian conference on Information Ethics took place in March 2010 at the Federal University of Paraiba (João Pessoa): http://dci.ccsa.ufpb.br/editais/SBEI.pdf See proceedings Freire 2010. See also Capurro 2010a.
314 For an overview on privacy in Latin America from the perspective of Western philosophy, dealing particularly with legal aspects of 'sensitive data', see Pfeiffer 2008. On Latin American cultures see Kusch 1962 and von Barloewen 1992.
315 See the portals RELEI (*Red Latinoamericana de ética de la información*) http://redeticainformacion.ning.com and *Red Universitaria de ética en el ciberespacio* http://www.redciberetica.org. See also the international seminar on privacy and data protection at the *First Brazilian Internet Forum* São Paulo, 13-14 October 2011. http://forumdainternet.cgi.br
316 MISTICA (*Metodología e Impacto Social de las Tecnologías de Información y Comunicación en América* – Methodology and Social Impact of Information and Communication Technologies in America) 2002 at http://www.funredes.org/mistica/english/project/ The following quotes are from this document at http://www.itu.int/wsis/docs/pc2/misc/mistica.doc. For a history of MISTICA see Pimienta 2007.

All these questions deal with privacy issues, not only with regard to the protection of locally produced knowledge, but especially protection of the communities or selves that produce such knowledge as being a genuine expression of their cultural identity. This is also underscored by the next point (6) "On the social change produced by the Internet" addressing the following issues:

"a. In what way do the actions which are promoted for the development of the Internet prompt elements such as development of personal and collective self-esteem, community organization, improvement of educational standards, capacities of interaction between people, empowerment, or development of the capacity to make proposals from the people with whom the work is done?
b. In what way are actions for the development of the Internet transforming the daily lives of the peoples, from an individual, occupational, interpersonal or citizen viewpoint?
c. What level of probability is there that the transformations produced by the actions that are carried out have a follow-up in the future?"

It is evident – at least from the concept of privacy developed within the present study on Digital Whoness – that issues around the "development of personal and collective self-esteem" are genuine privacy issues, even if they are not addressed as such. It is also apparent that privacy issues as issues of the self cannot be solved on an abstract level, but must be addressed by individuals and societies within the specific framework of their historical, and particularly indigenous, roots, experiences, aspirations and opportunities that stakes out how they play their who-games.

2.5.4 AFRICA[317]

The African philosopher, Mogobe Ramose, maintains that *ubuntu* is "the central concept of social and political organization in African philosophy, particularly among the Bantu-speaking peoples. It consists of the principles of sharing and caring for one another."[318] Ramose interprets two maxims "to be found in almost all indigenous African languages," namely: "*Motho ke motho ka batho*" and "Feta kgomo tschware motho". The first maxim means that "to be human is to affirm one's humanity by recognizing the humanity of others and, on that basis, to establish humane respectful relations with them. Accordingly, it is *ubuntu* which constitutes the core meaning of the aphorism." The second maxim signifies, "that if and when one is faced with a decisive choice between wealth and the preservation of life of another human being, then one should opt for the preservation of life."[319]

A detailed analysis of the relationship between *ubuntu* and privacy was provided by Olinger et al. at the Sixth International Conference on Computer Ethics: Philosophical Enquiry in 2005. They write, "The African worldview driving much of African values and social thinking is 'Ubuntu'" (Broodryk, 2004). The Ubuntu worldview has been recognized as the primary reason that South Africa has managed to successfully transfer power from a white minority government to a majority-rule government without bloodshed (Murithi, 2000). The South African government will attempt to draft a Data Privacy Bill and strike an appropriate balance within the context of African values and an African worldview."[320] According to Broodryk, *ubuntu* is an African worldview "based on values of intense humaneness, caring, respect, compassion, and associated

317 The following analysis reproduces some of the ideas and findings in Capurro 2007. For an overview of past, present and future activities in the field of information ethics in Africa, see Capurro 2010b.
318 Ramose 2002, p. 643.
319 Ramose 2002, p. 644.
320 Olinger et al. 2005, p. 292.

values ensuring a happy and qualitative human community life in a spirit of family."[321] In a comparative study of ethical theories in different cultures, Michael Brannigan addresses African ethics under the heading "To Be is to Belong."[322] Olinger et al. write, "Human beings are recognised as being all equal, sharing a common basic brotherhood, having the right to life and finding their ultimate meaning and purpose within communities. The last attribute is in stark contrast to the extreme individualism and self-centredness of Western cultures."[323] African whoness, at least from the *ubuntu* perspective, is rooted in community and not based on isolated, worldlessly encapsulated individuals. The *ubuntu* core values are communalism and interdependence. They are the basis for humaneness, caring, sharing, respect and compassion.[324]

The authors state that, "during the extensive literature review privacy was not explicitly mentioned anywhere among the Ubuntu writings."[325] This is easy to understand if privacy is conceived as pertaining to an isolated individual in which case, "[...] personal privacy would rather be interpreted as 'secrecy'". This "secrecy would not be seen as something good because it would indirectly imply that the Ubuntu individual is trying to hide something instead of protecting something – namely his personhood."[326] Clearly, the protection of *ubuntu*-personhood is not understood as privacy protection, nor is ubuntu culture itself oriented toward openness and transparency of an originary being-together in a common world according to the saying, "*Umunto ungumuntu ngabanye abantu*" (Nguni languages of Zulu and Xhosa), which means "A person is a person through other persons."[327]

Africa is culturally a complex continent. The issue of privacy in Africa from an ethical and intercultural perspective is only now being put on the agenda. This applies especially to the Arab countries in North Africa.

2.5.5 CONCLUSION

Homi Bhabha, director of the Humanities Center at Harvard University, has proposed a "global ethics that extends 'hospitality' to all those who lost their place where they belong due to an historical trauma, injustice, genocide or death".[328] Privacy understood from the perspective of whoness in the digitized cyberworld calls for an ethics of reciprocal hospitality, not only with regard to diverse ethical norms and principles, but also with regard to those who are marginalized in a global society in which digital technology has a dominating presence. Intercultural information ethics adopts a critical stance toward all kinds of destruction of the human habitat in the world, particularly such ways of thinking and life-practices that exclude others from their use or impose on them a particular way of playing out the interplay of whoness, thus thwarting their becoming free selves.

The thoughtful and practically oriented search for common values and principles should not overlook or 'forget' the complexity and variety of human cultures that are a genuine expression of humaneness, and not something to be overcome. This concerns, in particular, the notion of privacy conceived as what is proper to human self-understanding in being able to withdraw from others' gaze and lead one's

321 Broodryk 2002. On "African communalism" see the study of the Nigerian philosopher Simeon Eboh (Eboh 2004).
322 Branningan 2005.
323 Olinger et al. 2005, p. 294.
324 As presented in 2.2.6, and on a more abstract plane of sociation, even the reified gainful game of capitalism is open to a re-interpretation, and hence an alternative lived ethos, if reification itself is seen through and 'taken back', and earning a living itself is seen to be originarily – in the open clearing of a shared world – a mutual valuing of and caring for one another.
325 Olinger et al. 2005, p. 296.
326 Olinger et al. 2005, p. 296.
327 Olinger et al. 2005, p. 293.
328 Bhabha 2007, p. 44 (my translation, RC). On the Humanities Center at Harvard University see http://www.fas.harvard.edu/~humcentr/about/homi.shtml

own life shared with certain freely chosen others. An intercultural view of privacy must pay attention to what is in-between cultures, allowing the individually and socially moulded self to transform and enrich its identity through the cultural interplay both within and between cultures.

2.6 ETHICAL ISSUES AROUND THE CYBERWORLD AND PRIVACY IN CONNECTION WITH BASIC EU VALUES AND PRINCIPLES

Daniel Nagel

2.6.1 EUROPEAN INTEGRATION, FREEDOM, ECONOMICS

Freedom has always been a central principle in modern day Western democracies. Based on this legacy, European integration, which was initiated by traditionally Western states, was naturally centred thereon. This can be seen from the fact that when the European states set out for the first time to define basic common fundamental principles, all of them related to an area within the broad gamut of freedom. The free movement of persons, goods, services and capital was defined as the core of European co-operation.

Arguably, this freedom does not mirror the classical understanding of freedom as delineated, for instance, in the U.S. Bill of Rights. Nevertheless, the latter rights were established against a considerably different background. In 1789, the First U.S. Congress assembled and discussed for the first time the recently enacted Constitution, which in turn was written at a time when the independence of the states was still in its infancy. The Bill of Rights thus addressed issues the representatives thought were of utmost importance and should be taken into consideration: after having established general guiding principles on the new order, the common desire was to protect individuals from an abuse of power by the newly created government.[329] The Bill of Rights thus had the objective of securing fundamental freedoms of the citizens of an independent state.[330] Thus, the first amendment to be accepted stated that Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the Government for a redress of grievances.[331] Hence, the Congress clearly intended to safeguard the development and exercise of the recently gained liberty from interference. Thus, it explicitly listed the freedom of selves to determine their religious beliefs, to express their opinions in oral and written form and to interact with other selves. The First Amendment consequently is a collection bin of ethical core values (cf. *2.2.3 Values, ethos, ethics*) that are deemed necessary for a free democratic society from a traditionally Western point of view. The principles therefore can be seen as the basic foundation that needs to be present before secondary aspects such as the free movement of goods can be addressed. However, as these fundamental preconditions had already been present within the national legislations of the European member states who were to agree on co-operation, such aspects were not at the centre of attention but were covered by needs and challenges which had arisen in respect to cross-border transactions. Thus, European co-operation manifests predominantly an economic drift. This phenomenon can further be explained if the historical background of the European member states is taken into account, above all the World Wars, when

[329] Cf. Preamble to the Bill of Rights dated 4 March 1789: "The Conventions of a number of the States, having at the time of their adopting the Constitution, expressed a desire, in order to prevent misconstruction or abuse of its powers, that further declaratory and restrictive clauses should be added: And as extending the ground of public confidence in the Government, will best ensure the beneficent ends of its institution."

[330] Interestingly, the only two amendments that were rejected by the First Congress were amendments that were of a mere procedural nature: the redistribution of constituents.

[331] Cf. Amendment 1 of the Bill of Rights dated 4 March 1789.

neighbouring states seemed to have turned into irreconcilable enemies. Following the atrocities and deep wounds inflicted, it was far easier for the member states to find economic compromises first since they shared common economic needs which could be addressed without opening up old wounds. Despite the fact that the states involved were located on the same continent and had many similarities in their roots and traditions, an assimilation of fundamental policy principles proved to take much longer – and required outside factors to be catalysed.

Consequently, European integration was pushed from the very beginning from an economic perspective. When France, Italy, Germany, Belgium, the Netherlands and Luxemburg signed the ECSC treaty in 1951, the main objective was to establish a common market in coal and steel.

A year later, the European Defence Community was created to counter emerging tensions between East and West. The sword of Damokles of a potential new World War forced western European states to overcome differences and mistrust, and also boosted the existing will to co-operate. If it had not been for a French veto in 1954, the member states would have agreed on very close political co-operation at a very early stage which would have shifted the focus from mere economic issues to finding political consensus in many fields, including law and politics.

As a consequence, the continuing integration efforts, such as the Euratom Treaty and the EEC Treaty in 1957 reverted to a purely economic focus.

In the 1970s the Davignon Report was released. The latter provided for quarterly meetings of foreign ministers and the establishment of a permanent political secretariat.

The initial enlargement of the European Community in the late seventies and eighties led to a rebirth of the quest for common European aims. Nevertheless, not until the Iron Curtain was about to fall and more member states joined the Community (which was renamed at that very time), the focus finally shifted from foreign politics and the striving to guarantee the best possible level of military security to internal objectives, and finally to citizens.

2.6.2 THE EUROPEAN CONVENTION FOR THE PROTECTION OF HUMAN RIGHTS AND FUNDAMENTAL FREEDOMS

In 1950 the European Convention for the Protection of Human Rights and Fundamental Freedoms laid down clear standards for what was considered worthy of protection.[332] This convention was tailored to the needs of people in a century of wars, persecution and oppression. It focused on the victims of these catastrophes, the people. The founding fathers set out to create a binding scheme for a common and conclusive protection of individuals.[333] Consequently, the Preamble stresses the joint ethical values that united and led the parties to the Convention to agree on a joint document by highlighting that the provisions would represent the common traditions and ideals of the signatories to the Convention. With regard to the founding fathers, these traditions were clearly of a traditional western European nature, albeit the Convention latter proved to be also acceptable for states that do not share the traditional Western background.[334] The core of these values is composed of the protection of fundamental human rights such as the right to life, the prohibition of torture, slavery and liberty as well as additional fundamental freedoms.

---

332 European Convention on Human Rights, Rome 4 November 1950.

333 At that time the Convention was established by the governments of the Kingdom of Belgium, the Kingdom of Denmark, the French Republic, the Irish Republic, the Italian Republic, the Grand Duchy of Luxembourg, the Kingdom of the Netherlands, the Kingdom of Norway, the Kingdom of Sweden and the United Kingdom of Great Britain and Northern Ireland.

334 Cf. e.g. the ratification of the Convention by Russia in 1998 and Azerbaijan in 2002.

The European Convention for the Protection of Human Rights and Fundamental Freedoms for the first time contained a safeguard for its implementation in practice. It both provided for a Commision that administrated complaints and – more notably – a Court to oversee the adherence of member states to the Convention. Finally, the rights set out by the Convention are not only a set of passive rights that can be invoked when an infringement is made, but also a positive obligation on member states to guarantee an automatic minimum level of protection.[335]

These basic rights mirrored the quest to end years of atrocities and war crimes and to clearly demonstrate the intent to treat and protect individuals, irrespectively of their nationality, race or ethnicity. The European Convention for the Protection of Human Rights and Fundamental Freedoms not only introduced these very basic principles, but also established a scheme to safeguard additional freedoms centring on the self, its free development and the potential to freely interact with other selves.

Notably, the right to demand respect for private and family life is the first right that is mentioned which does not refer to bodily integrity and liberty, but to the freedom of the self to choose how and when to interact with other selves in a shared world. Article 8 states that "(e)veryone has the right to respect for his private and family life, his home and his correspondence." Thus, not only the private sphere in a personal, spatial sense but also in respect to the interplay with other selves is regarded as a fundamental value of human rights. Section two of this Article delineates a major safeguard in this respect, but also an erosion of that very right, namely, that "there shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others."

The limitation of the self's freedom to choose when, how and what to conceal and reveal is thus made subject to and qualified by security interests of the state. This arguably entails the danger of undermining the right to determine the spectrum of what to reveal or conceal depending on the context in which the self finds itself situated, since it leaves a back door open to invoke security issues in many contexts as a pretence to curtail this right to privacy.

When the following Articles are examined, it can be seen how the notion of privacy was further understood. Articles 9 and 10 of the European Convention for the Protection of Human Rights and Fundamental Freedoms guarantee the freedom of thought and expression. This is the basis of a free interplay among self-determined selves since only the ability to freely express oneself allows also for a free interaction. As long as a self is guaranteed the freedom to deliver its thoughts to other selves without restrictions on content or form s/he is able not only to develop and shape its character, but also to foster a viable, fluid society through free interplay with others of his kind. Only such pluralistic interplay, in turn, is capable of bolstering the precondition mentioned in the Preamble, namely, a free democratic state. Both freedom of thought and freedom of expression, however, are also qualified; both are subject "to such limitations as are prescribed by law and are necessary in a democratic society in the interests of public safety, for the protection of public order, health or morals, or for the protection of the rights and freedoms of others." While a basic limitation can be seen as generally necessary to be able to guarantee equal protection of all selves, thus supporting a free interplay which neither allows for an imbalance nor for a certain stage direction to be followed, this exception also manifests a dilution of the proclaimed freedoms.

[335] Cf. e.g. McCann and others vs. United Kingdom, Eur. Ct. HR (1995) 21 EHRR 97.

The freedom of thought and expression is rounded off by a guarantee of the freedom of assembly in Article 11. This freedom is a basic requirement to enable a free interplay among selves and to prevent a focus on an individual, encapsulated self.

In conclusion, the 1950 European Convention for the Protection of Human Rights and Fundamental Freedoms already painted a clear picture with respect to the ethical values of living underlying European policy as regards privacy: the core of protection is a self who shall be free to determine its interaction or non-interaction with others.

2.6.3 THE INTERNATIONAL COVENANT ON CIVIL AND POLITICAL RIGHTS

In 1966 the United Nations furthered international legislative measures to secure the fundamental freedoms of persons and drafted the International Covenant on Civil and Political Rights.[336] It came into force on 23 March 1976. This Covenant had a slightly different weighting. While the main emphasis of the European Convention for the Protection of Human Rights and Fundamental Freedoms clearly was on the protection of individuals against interference from governments, the Covenant on Civil and Political Rights stressed personal freedom of the self:[337] Article 1 provides that all peoples have the right to self-determination. It further enunciates in phrase 2 that "by virtue of that right they freely determine their political status and freely pursue their economic, social and cultural development". This attempt to enshrine free self-determination on an international basis can be seen as remarkable at a time when equality still was a newly introduced term in many states that were considered to be progressive.[338] Article 1 mirrors a broad understanding of the notion of self-determination. On the one hand, it shows that self-determination involves both the ability to freely determine of one's own volition without influence or interference by third parties or authorities, and the ability to decide about one's self.

The Covenant on Civil and Political Rights does not proclaim an unqualified right, but allows also for limitations under certain circumstances. Article 4 of the Covenant provides for exceptional cases in which states might deviate from the guaranteed right to free self-determination: Nevertheless, it is explicitly stated that such deviation is only admissible if it does not constitute a discriminatory measure.

Arguably, the Covenant on Civil and Political Rights can still be seen as a watchdog with soft, wiggly teeth since enforcement is dependent on the willingness of sovereign states to oblige themselves to really keep to a strict interpretation close to the wording. Nevertheless, there is not only a negative aspect to the limitation. It also shows an embodiment of the fact that the right to self-determination cannot be seen solely as the right of an isolated subject alienated from the outside world.

2.6.4 THE COUNCIL OF EUROPE RESOLUTION ON THE PROTECTION OF THE PRIVACY OF INDIVIDUALS VIS-À-VIS ELECTRONIC DATA BANKS IN THE PRIVATE AND PUBLIC SECTORS

The Committee of Ministers of the Council of Europe started in the seventies to shift the focus from a more general

336 Adopted and opened for signature, ratification and accession by General Assembly resolution 2200A (XXI) dated 16 December 1966, available at: http://www2.ohchr.org/english/law/ccpr.htm. The Covenant has been signed or ratified by 74 states up to the present day including most European states, the U.S., China and Russia.

337 The right to life, the protection from torture and slavery, liberty and equality before the law follow in Part III of the Covenant.

338 Cf. e.g. the end of segregation in the U.S. which is often linked to the case Brown v. Board of Education of Topeka, (347 U.S. 483 (1954)) in the mid-fifties, or the fact that many European states (e.g. France, Italy Belgium) only introduced the right for women to vote in the late forties, Switzerland not until 1971.

appreciation of the protection of individual free self-determination and privacy to a more specific protection in certain circumstances. It issued two Resolutions for this purpose, the Resolution on the protection of the privacy of individuals vis-à-vis electronic data banks in the private sector[339] and the Resolution on the protection of the privacy of individuals vis-à-vis electronic data banks in the public sector.[340] Both Resolutions stressed the need for prevention of abuses in the storing, processing and dissemination of personal information by means of electronic data banks as well as the importance of finding a joint international approach. In addition, both resolutions are more directed at data controllers than at the individual data subject. Consequently, they serve as additional armory for the fundamental principles set out by the European Convention for the Protection of Human Rights and Fundamental Freedoms in a changed world, where data storage no longer refers only to dusty filing cabinets but comprises the transformation of information into electronic bit-strings that render both the filing specialist and index cards superfluous.

The Resolution on the protection of the privacy of individuals vis-à-vis electronic data banks in the private sector defines the framework within which collection and storage of data through electronic data banks can be admissible. It already sets out clear boundaries for such collection and storage as well as defining basic principles such as, in particular, the principle of data quality: Article 1 of the Annex of the Resolution provides that data should be accurate, kept up to date and not recorded or disseminated if this might lead to unfair discrimination. In addition, it also introduced the collection and use-limitation principle,[341] the purpose-specification principle[342] as well as cautious attempts at security, accountability and even transparency.[343] These principles can be found in many subsequent legislative approaches to the protection of data and privacy.[344]

The Resolution on the protection of the privacy of individuals vis-à-vis electronic data banks in the public sector in turn strengthens the defense against intrusion and infringement of personal privacy through the state. It is drafted against the backdrop of the recognition that the use of electronic data banks by public authorities has given rise to increasing concern about the protection of the privacy of individuals.

2.6.5 THE CONVENTION FOR THE PROTECTION OF INDIVIDUALS WITH REGARD TO AUTOMATIC PROCESSING OF PERSONAL DATA AND THE OECD GUIDELINES ON THE PROTECTION OF PRIVACY AND TRANSBORDER FLOWS OF PERSONAL DATA

In 1981 the Council of Europe laid out the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data.[345] According to its Preamble, this convention aims at creating greater unity in the dissmeniation of the rule of law, human rights and fundamental

339 Resolution (73) 22 of the Council of Europe, adopted by the Committee of Ministers on 26 September 1973 at the 224th meeting of the Ministers' Deputies.

340 Resolution (74) 29 of the Council of Europe Adopted by the Committee of Ministers on 20 September 1974 at the 236th meeting of the Ministers' Deputies.

341 Article 2 provides that "the information should be appropriate and relevant with regard to the purpose for which it has been stored."

342 Cf. Article 5 "Without appropriate authorisation, information should not be used for purposes other than those for which it has been stored, nor communicated to third parties".

343 Cf. Article 6 a general rule, the person concerned should have the right to know the information stored about him, the purpose for which it has been recorded, and particulars of each release of this information.

344 Cf. e.g. Article 6 of the Directive (EC) 95/46 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 [1995] OJ L281/31.

345 Convention No. 108 dated 28 January 1981 (http://conventions.coe.int/treaty/en/treaties/html/108.htm).

freedoms as well as the engendering of unity among member states. This reference clearly addresses loopholes left by the European Convention for the Protection of Human Rights and Fundamental Freedoms and developments which had eventuated since it came into force. Hence, the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data was not intended as another broad compromise on fundamental principles. It neither ventured to lay down new rights; rather, it was drafted to address new challenges to the existing protection of individuals and their privacy which arose during the course of an increase in surveillance, identity-recognition, distribution and storage systems by virtue of a rapid development of the technical means employed. While traditionally threats to privacy could be located in the immediate surroundings of a self and could thus be controlled by the self and its governments, through conscious decisions on carrying out and protecting the play of concealing and revealing information, these threats were taken to a next level by digitization. Information and acts that relate to a self and were considered private in the sense of belonging to a personal world where the self should be free to determine whether they should be disclosed or kept secret started to be economically valuable and roused the interest of more and more third parties. It also became easier to access and collect such data thanks to the dawn of the electronic information age. Finally emerging globalization also took its stake in the economic striving for gain.

The drafting process of this Convention involved close cooperation with the masterminds behind the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data which were published a year earlier.[346] The OECD set-up – while establishing comparable general rules – differed slightly from the Council Convention by putting the main emphasis on transborder flows and automated treatment of data.

The Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data states that its objective is to secure "for every individual [...] respect for his rights and fundamental freedoms, and in particular his right to privacy". Thus first and foremost, the self is to be protected. If compared to the Council Resolutions (see 2.6.4 above), there is a shift from being the mere object of protection to being the starting-point for any consideration of what is worthy of protection. This shift has to be applauded since privacy should be understood not only as a merely defensive right as in the case of the right to be left alone.[347]

The Convention includes both a definition of what is to be considered as personal data and an enumeration of basic principles which need to be respected.[348] It also contains a first attempt at securing these principles by defining a subject who is responsible for handling the data.[349] The basic principles set out represent a remarkable multi-faceted nutshell approach or, in Greenleaf's words, these principles "while stated briefly, do contain versions of most of the elements we now recognise as core data privacy principles".[350]

The main principle laid out by the Convention concerns the quality of data.[351] This principle sets out the requirements for fair and lawful processing on the basis of specified,

346 OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data dated 23 September 1980 (http://www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,00.html)

347 Cf. for instance the dissenting opinion of Justice Brandeis in *Olmstead v. United States*, 277 U.S. 438 (1928), who delineated the scope of this right as "every unjustifiable intrusion by the Government upon the privacy of the individual, whatever the means employed, must be deemed a violation of the Fourth Amendment".

348 Personal data are specified as "any information relating to an identified or identifiable individual". This definition can be found also in the first part the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data dated 23 September 1980.

349 Cf. Article 2: "controller of the file" means "the natural or legal person, public authority, agency or any other body who is competent according to the national law to decide what should be the purpose of the automated data file, which categories of personal data should be stored and which operations should be applied to them".

350 Greenleaf 2012.

351 Cf. Article 5 of the Convention.

legitimate purposes with regard to adequacy and relevance for the respective purpose, as well as accuracy and a limitation of the storage-period to the necessary minimum. As even a financial, taxation interest of the state can form the basis for severely exceeding the limitation for data collection and storage to a minimum, it might be asked whether the Convention is a well-intentioned but toothless tiger. To put it differently, this exception entails the danger that the mere economic value of data is more highly appreciated than the who from whom such data originate.

Nevertheless, the Convention contains a further fundamental milestone: Article 6 defines a basis for qualifying data.[352]

Notwithstanding the unfortunate back door which might endanger the intended scope of protection, the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data can still be seen as a regulatory success. It has been ratified by forty-four member states of the Council of Europe so far, all of which have privacy laws and thus, at least, have acknowledged that privacy is a core value for living worthy of protection.

2.6.6 CONCLUSION – A WATERTIGHT APPROACH?

The European Convention for the Protection of Human Rights and Fundamental Freedoms, the International Covenant on Civil and Political Rights and the Council of Europe Resolutions on the protection of the privacy of individuals vis-à-vis electronic data banks in the private and public sector as well as the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data all spread out a basic safety net for the self. Nevertheless, in particular, the exceptions woven in allowing deviations and derogations show that not only the interests of the selves concerned (citizens living their private lives), but also strong economic interests as well as the interest of the contracting states to conserve power, including the power of taxation, were considered when the various principles were laid down.

When freedom is held to be a treasured, indispensable quality of social life, both individual freedom and the joint freedom of selves in interplay, irrespectively of viewing angle, need to be upheld and secured by legal instruments.

The European Union has proclaimed such freedoms within its fundamental common principles of freedom, notably with respect to the free movement of goods, persons, services and capital.[353] The European Union further delineated this with respect to personal privacy in a landmark attempt to harmonize data protection, European Directive 95/46.[354] This directive (re)introduced another important principle, the so-called principle of consent.[355] If it had not been for several exceptions to this principle,[356] the focus would have finally shifted to the true starting-point for any protection, namely, people themselves. At least

352 Article 6 reads "Personal data revealing racial origin, political opinions or religious or other beliefs, as well as personal data concerning health or sexual life, may not be processed automatically unless domestic law provides appropriate safeguards. The same shall apply to personal data relating to criminal convictions."

353 Cf. the Treaty Establishing the European Community, Title I and Title III dated 25 March 1957.

354 Directive (EC) 95/46 of the European Parliament and of the Council dated 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L281/31.

355 Cf. the Preamble "Whereas, in order to be lawful, the processing of personal data must in addition be carried out with the consent of the data subject [...]" and Article 7 "Member States shall provide that personal data may be processed only if: the data subject has unambiguously given his consent [...]" of Directive (EC) 95/46.

356 Article 7 also allows for data collection in the case of necessity for the performance of a contract, for compliance with a legal obligations, to protect the vital interests of the data subject, for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller and also for the purposes of legitimate interests pursued by the controller or by a third party or parties, to whom the data are reasonably disclosed.

this directive no longer allows for justifying a limitation of privacy on the basis of vague rules, but clearly stipulates the only contexts within which a deviation is permissible.

In 2003 the European Union again showed its willingness to finally enshrine fundamental principles in a way that would have created inalienable fundamental rights for any citizen of the member states all over Europe by drafting a Charter of Fundamental Rights within a European Convention.[357]

The 2009 Lisbon Treaty saved the Charter, albeit by giving it only the same status as the basic treaties, and not the legal force a Constitution would have had.[358] Nevertheless, the European quest to find the best way to protect the freedom and privacy of its citizens does not end here.[359] The Union tries to keep pace with technological developments, even if, due to continuing technological and other developments in the cyberworld, this might seem Sisyphean. The European Union still has to be encouraged and applauded – after all, it is the freedom of selves and thus our own freedom that is at stake.

LITERATURE

Adams et al. 2009
Adams, Andrew, Kiyoshi Murata & Yohko Orito 'The Japanese Sense of Information Privacy' in *AI & Society* Vol. 24 2009 pp. 327-341. Available at http://www.springerlink.com/content/708886t6482g3v62/fulltext.pdf

Adams et al. 2011
Adams, Andrew, Kiyoshi Murata, Yohko Orito and Pat Parslow 'Emerging Social Norms in the UK and Japan on Privacy and Revelation in SNS' in *International Review of Information Ethics Vol. 16 2011*.

Amino 1996
Amino, Yoshihiko *Muen, Kugai,Raku* Tokyo, Heibonsha 1996.

Ariès & Duby 1985/1989
Ariès, Philippe & Georges Duby (eds.) Geschichte des privaten Lebens (ed.) Paul Veyne, translated by Holger Fliessbach 3rd ed. Hamburg: Fischer 1989 (original: Histoire de la vie privée Paris: Seuil 1985). I. Band *Vom Römischen Imperium zum Byzantinischen Reich*.

Aristotle Met.
Aristotle *Metaphysics* in *Works in Twenty-Three Volumes* Vols. XVII & XVIII Loeb Classical Library, Harvard U.P. and W. Heinemann, London 1938ff.

Aristotle Eth. Nic.
Aristotle *Nicomachean Ethics* in *Works* Vol. XIX.

Aristotle Phys.
Aristotle *Physics* in *Works* Vols. IV and V.

Aristotle Pol.
Aristotle *Politics* in *Works* Vol. XXI.

357 Cf. in particular Chapter II of the Charter of Fundamental Rights (2000/C 364/01) which formulates the protection of individual freedoms as absolute rights without mentioning within the same Chapter any potential room to deviate.

358 Cf. Article 6 of the Treaty of Lisbon amending the Treaty on European Union and the Treaty establishing the European Community, signed at Lisbon, 13 December 2007, 2007/C 306/01: "The Union recognises the rights, freedoms and principles set out in the Charter of Fundamental Rights of the European Union of 7 December 2000, as adapted at Strasbourg, on 12 December 2007, which shall have the same legal value as the Treaties."

359 Cf. the draft of the 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) of 25 January 2012, COM(2012) 11 final.

Arendt 1958/1998
Arendt, Hannah *The Human Condition* 2nd ed. with an introduction by Margaret Canovan, Chicago U.P. 1998, 1st ed. 1958.

Augustine Confessiones
Augustine *Confessiones*, many editions.

Baasch-Andersen 2011
Baasch-Andersen, Camilla 'Noblesse Oblige ...? Revisiting the Noble Month and the Expectations and Accomplishments it has prompted' *Festschrift for Ingeborg Schwenzer Private Law national – global – comparative* Bd. I & II, XXIII Stämpfli Verlag AG, Bern 2011.

Barrán et al. 1996
Barrán, José Pedro, Gerardo Caetano & Teresa Porzecanski (eds.) *Historias de la vida privada en el Uruguay* Montevideo: Taurus 1996ff.

Beavers 2002
Beavers, Anthony F. 'Phenomenology and Artificial Intelligence' in *CyberPhilosophy: The Intersection of Philosophy and Computing* James H. Moor and Terrell Ward Bynum (eds) Oxford: Blackwell 2002 pp. 66-77. Also in *Metaphilosophy* Vol. 33.1/2 2002 pp. 70-82.

Bernstein et al. 2009
Bernstein, Daniel J., Johannes Buchmann & Erik Dahmen (eds) *Post-Quantum Cryptography* Berlin/Heidelberg: Springer 2009.

Bhabha 2007
Bhabha, Homi K. 'Ética e Estética do Globalismo: Uma Perspectiva Pós-Colonial' in Fundaçao Calouste Bulbenkian and Fórum Cultural O Estado do Mundo (eds.) *A Urgência da Teoria* Lisboa: Ed. Tinta-da-china 2007 pp. 21-44.

Bien 1985
Bien, Günther *Die Grundlegung der politischen Philosophie bei Aristoteles* Freiburg: Karl Alber Verlag, 1985.

Brannigan 2005
Brannigan, Michael C. *Ethics Accross Cultures with Power-Web Ethics* New York, McGraw-Hill 2005.

Brey 2007
Brey, Philip 'Global Information Ethics and the Challenge of Cultural Relativism' in *European regional Conference on the ethical dimensions of the information society* 2007. Available at http://portal.unesco.org/ci/en/ev.php-URL_ID=25455&URL_DO=DO_TOPIC&URL_SECTION=201.html

Broodryk 2002
Broodryk, Johann Ubuntu: *Life lessons from Africa* Ubuntu School of Philosophy, Pretoria 2nd ed. 2002.

Capurro 1978
Capurro, Rafael *Information: Ein Beitrag zur etymologischen und ideengeschichtlichen Begründung des Informationsbegriffs* Munich: Saur 1978

Capurro 1986
Capurro, Rafael *Hermeneutik der Fachinformation* Karl Alber Verlag, Freiburg 1986

Capurro 1995
Capurro, Rafael *Leben im Informationszeitalter* Berlin: Akademie Verlag 1995

Capurro 1999
Capurro, Rafael 'Digitaler Weltentwurf' 1999 available at www.capurro.de

Capurro 2001
Capurro, Rafael 'Beiträge zu einer digitalen Ontologie' 2001 available at www.capurro.de

Capurro 2003
Capurro, Rafael *Ethik im Netz* Stuttgart: Franz Steiner Verlag 2003

Capurro 2004/2008
Capurro, Rafael 'Between Trust and Anxiety. On the Moods of Information Society' in *Ethical Space: The International Journal of Communication* Vol. 2, No. 4, pp. 18-21 2004. Erschien auch in: Richard Keeble (ed.) *Communication Ethics Today* Leicester: Troubadour Publ. 2005, pp. 187-196. (Deutsche Übersetzung 'Zwischen Vertrauen und Angst. Über Stimmungen der Informationsgesellschaft' in D. Klumpp, H. Kubicek, A. Roßnagel, W. Schulz (eds.) *Informationelles Vertrauen für die Informationsgesellschaft* Berlin, Heidelberg: Springer 2008 pp. 53-62.

Capurro 2005
Capurro, Rafael 'Privacy: An intercultural perspective' in *Ethics and Information Technology* Vol. 7 pp. 37-47: Online: http://www.capurro.de/privacy.html 2005.

Capurro 2006
Capurro, Rafael 'àsdf ' in Tassilo Pellegrini, Andreas Blumauer (eds.) *Semantic Web. Wege zur vernetzten Gesellschaft* Springer, Berlin 2006

Capurro 2007
Capurro, Rafael 'Information Ethics for and from Africa' in *International Review of Information Ethics* Vol.7 2007. Available at http://www.i-r-i-e.net/inhalt/007/01-capurro.pdf

Capurro 2008
Capurro, Rafael 'Intercultural Information Ethics' in Kenneth E. Himma and Herman T. Tavani (eds.) *The Handbook of Information and Computer Ethics* New Jersey, Wiley 2008 pp. 639-665. Available at http://www.capurro.de/iiebangkok.html

Capurro 2009
Capurro, Rafael 'Etica intercultural de la información' in Henriette Ferreira Gomes, Aldinar Martins Bottentuit, Maria Odaisa Espinheiro de Olivera (eds.) *A ética na sociedade, na área da informação e da atuação profissional* Brasilia DF, Conselho Federal de Biblioteconomia 2009 pp. 43-64. Available at http://www.capurro.de/reforma.html

Capurro 2009a
Capurro, Rafael 'Leben in der *message society*. Eine medizinethische Perspektive' Beitrag zum Kongress FORUM Medizin 21 *Ärztin / Arzt sein im 21. Jahrhundert. Erwartung, Selbstbild, Realität* Salzburg. Online: http://www.capurro.de/paracelsus.html 2009.

Capurro 2009b
Capurro, Rafael 'Ethik der Informationsgesellschaft. Ein interkultureller Versuch' in *Jahrbuch Deutsch als Fremdsprache – Intercultural German Studies* Bd. 35 iudicium Verlag, München 2009 pp. 178-193. http://www.capurro.de/parrhesia.html

Capurro 2009c
Capurro, Rafael 'Ethics and Robotics' in R. Capurro und M. Nagenborg (eds.) *Ethics and Robotics* Akademische Verlagsanstalt, IOS Press, Heidelberg 2009 pp. 117-123. Online: http://www.capurro.de/ethicsandrobotics.html

Capurro 2009d
Capurro, Rafael 'Fremddarstellug – Selbstdarstellung. Über Grenzen der Medialisierung menschlichen Leidens' in Stefan Alkier und Kristina Dronsch (Hrsg.) *HIV/AIDS – Ethische Perspektiven. Proceedings der Interdisziplinären Fachtagung* Berlin: de Gruyter pp. 143-156. Available at http://www.capurro.de/aids.html 2009.

Capurro 2010
Capurro, Rafael 'Wandel der Medizin in digitalen Informationsgesellschaften' in *Imago Hominis. Quartalschrift für Medizinische Anthropologie und Bioethik* Bd. 17 Heft 2, 2010 pp. 97-104.

Capurro 2010a
Capurro, Rafael *Desafíos teóricos y prácticos de la ética intercultural de la información*. Keynote at the first Brazilian conference on Information Ethics, João Pessoa, Brazil 2010. Available at http://www.capurro.de/paraiba.html

Capurro 2010b
Capurro, Rafael I*nformation Ethics in Africa. Past, Present and Future Activities* (2007-2010) 2010. Available at http://www.capurro.de/wsis2010_africa_infoethics.html

Capurro 2010/2011
Capurro, Rafael *The Dao of the Information Society in China and the Task of Intercultural Information Ethics*. Beijing 2010 (Chinese translation by Julan Liang in *Social Sciences Abroad* 2011). Available at http://www.capurro.de/china_infoethics2010.html

Capurro 2011
Capurro, Rafael 'Never Enter your Real Data'. Online: http://www.capurro.de/realdata.html 2011.

Capurro & Capurro 2008
Capurro, Rafael & Capurro, Raquel 'Secreto, lenguaje y memoria en la sociedad de la información' [Geheimnis, Sprache und Gedächtnis in der Informationsgesellschaft] in pensardenuevo.org http://pensardenuevo.org/accion-en-la-red/especiales/secreto-lenguaje-y-memoria-en-la-sociedad-de-la-informacion/ Online: http://www.capurro.de/secreto.html 2008.

Capurro et al. 2007
Capurro, Rafael, Johannes Frühbauer & Thomas Hausmanninger (eds.) *Localizing the Internet. Ethical aspects in intercultural perspective* Munich. Fink 2007.

Capurro & Holgate 2011
Capurro, Rafael & Holgate, John (eds.) *Messages and Messengers. Angeletics as an Approach to the Phenomenology of Communication* Munich: Fink 2011.

Capurro & Nagenborg 2009
Capurro, Rafael & Nagenborg, Michael (eds.) *Ethics and Robotics* Heidelberg: Akademische Verlagsgesellschaft, IOS Press 2009.

Capurro & Nagenborg 2011
Capurro, Rafael and Nagenborg, Michael *ETICA Project, Deliverable 3.2.2. Ethical Evaluation*. Online: http://www.etica-project.eu/ 2011.

Capurro & Nakada 2009
Capurro, Rafael & Nakada, Makoto 'The Public / Private Debate. A Contribution of Intercultural Information Ethics' in Rocci Luppicini und Rebecca Adell (eds.) *Handbook of Research in Technoethics* Hershey NY, Information Science Reference 2 Vols. 2009, Vol. 1 pp. 339-353.

Capurro & Nakada 2011
Capurro, Rafael & Nakada, Makoto 'A Dialogue on Intercultural Angeletics' in *Contributions to Angeletics* Rafael Capurro and John Holgate (eds.) Munich: Fink 2011

Chalmers 2009
Chalmers, David J. 'Ontological Anti-Realism' in *Metametaphysics: New Essays on the Foundations of Ontology* Oxford: Clarendon Press 2009. http://consc.net/papers/ontology.pdf

Cicerchia 1998
Cicerchia, Ricardo *Historia de la vida privada en la Argentina* Buenos Aires: Troquel 1998.

Cooley 2011
Cooley, Thomas M. *Cooley On Torts* 29 (2nd ed. 1888), quoted in http://cyber.law.harvard.edu/privacy/Gormley–100%20Years%20of%20Privacy–%20EXCERPTS.htm accessed August 2011

Del Duca et al. 2008
Del Duca, Louis, Kritzer, Albert & Nagel, Daniel 'Achieving optimal use of harmonization techniques in an increasingly interrelated 21st century world – consumer sales: moving the EU harmonization process to a global plane' *UCCLJ* 2008 pp. 51-65.

Descartes 1996
Descartes, René *Regulae ad Directionem Ingenii* in *Philosophische Schriften* Meiner, Hamburg, 1996.

Devoto & Madero 1999
Devoto, Fernando & Marta Madero *Historia de la vida privada en la Argentina* Buenos Aires: Taurus 1999.

Dürmaier 2008
Dürmaier, Ana Thereza 'Ética Intercultural da Informação e Sustentabilidade. Kalagatos' in *Revista de Filosofia* Vol. 5, 9 2008 pp. 107-127. Available at http://www.uece.br/kalagatos/dmdocuments/V5N9_etica_intercultural_sustentabilidade.pdf

Eboh 2004
Eboh, Simeon Onyewueke *African Communalism. The Way to Social Harmony and Peaceful Co-Existence* Vol. 3 Onuganotu Lectures, Frankfurt, IKO Verlag für interkulturelle Kommunikation 2004.

Eldred 1984/2010
Eldred, Michael *Critique of Competitive Freedom and the Bourgeois-Democratic State: Outline of a Form-Analytic Extension of Marx's Uncompleted System* Kurasje, Copenhagen 1984, e-book edition www.arte-fact.org 2010. With an extensive bibliography.

Eldred 1996/2002
Eldred, Michael 'As: A Critical Note on David Farrell Krell's *Daimon Life*' www.arte-fact.org 1996/2002.

Eldred 1997/2010
Eldred, Michael *Worldsharing and Encounter: Heidegger's Ontology and Lévinas' Ethics* www.arte-fact.org Ver. 1.0 1997, Ver. 3.0 2010.

Eldred 1999
Eldred, Michael *Phänomenologie der Männlichkeit* Röll Verlag, Dettelbach 1999.

Eldred 2000/2010
Eldred, Michael *Kapital und Technik: Marx und Heidegger* Röll, Dettelback 2000; english version in *Left Curve* No. 24, May 2000; Ver. 3.0 www.arte-fact.org 2010.

Eldred 2008/2011
Eldred, Michael *Social Ontology: Recasting Political Philosophy Through a Phenomenology of Whoness* ontos, Frankfurt 2008; 2nd emended, revised, extended e-book edition, www.arte-fact.org 2011. With an extensive bibliography.

Eldred 2009
Eldred, Michael 'Anglophone Justice Theory, the Gainful Game and the Political Power Play' www.arte-fact.org 2009; also in Eldred 2008/2011.

Eldred 2009/2011
Eldred, Michael *The Digital Cast of Being: Metaphysics, Mathematics, Cartesianism, Cybernetics, Capitalism, Communication ontos*, Frankfurt 2009; emended, revised, extended e-book edition Ver. 3.0, www.arte-fact.org 2011. With an extensive bibliography.

Eldred 2010
Eldred, Michael 'Values, social and beyond' in *Indigo - Humanities Magazine for Young People* Vol. 3 Busan, South Korea 2010 pp. 34-45. Available at www.arte-fact.org

Eldred 2011a
Eldred, Michael *The Time of History: Hegel, Heidegger, Derrida, Marx* www.arte-fact.org Ver. 1.0 2011.

Eldred 2011b
Eldred, Michael 'Circulating Messages to Every Body and No Body' in Rafael Capurro & John Holgate (eds.) *Messages and Messengers: Angeletics as an Approach to the Phenomenology of Communication* Fink, Paderborn 2011 pp. 113-123.

Eldred 2012
Eldred, Michael *Out of your mind? Parmenides' message* www.arte-fact.org Ver. 1.0 2012.

Eldred 2012a
Eldred, Michael 'Interview „Zeit und Beschleunigung"' in *Newsletter des Frankfurter Forum für Altenpflege* März 2012 (http://www.ffa-frankfurt.de/241-pm-akl-2012-03-20.html).

Eldred 2012b
Eldred, Michael 'Turing's cyberworld of timelessly copulating bit-strings' www.arte-fact.org Ver. 1.0 2012.

Ess 2005
Ess, Charles 'Lost in translation? Intercultural dialogues on privacy and information ethics. Introduction to special issue on Privacy and Data Privacy Protection in Asia' in *Ethics and Information Technology* Vol. 7 2005 pp. 1-6.

Ess 2006
Ess, Charles 'Ethical pluralism and global information Ethics' in *Ethics and Information Technology* Vol. 8 2006 pp. 215-226.

Ess 2008
Ess, Charles 'Culture and Global Networks. Hope for a Global Ethics?' in Jeroen van den Hoven and John Weckert (eds.) *Information Technology and Moral Philosophy* Cambridge U.P. 2008 pp. 195-225.

Ess 2009
Ess, Charles 'Floridi's Philosophy of Information and Information Ethics: Current Perspectives, Future Directions' in *The Information Society* Vol. 25 2009 pp. 159–168.

Ess 2010
Ess, Charles *Digital Media Ethics*. Malden MA, Polity Press 2010.

Fink 2010
Fink, Eugen *Spiel als Weltsymbol* Cathrin Nielsen & Hans Rainer Sepp (eds.) Freiburg/Munich: Alber Verlag 2010.

Floridi 1999
Floridi, Luciano *Philosophy and Computing: An Introduction* New York: Routledge 1999.

Floridi 2006
Floridi, Luciano 'Four challenges for a theory of informational privacy' in *Ethics and Information Technology* 8(3) 2006 pp. 109–119. Accessed August 2011 at http://www.philosophyofinformation.net/

Floridi 2006a
Floridi in *Ethics and Information Technology* 8(3) 2006 pp. 1–16. Accessed August 2011 at http://www.philosophyofinformation.net/Articles.html

Floridi 2008
Floridi, Luciano 'Information ethics: A reappraisal' in *Ethics and Information Technology* 10(2–3) 2008 pp. 189–204.

Floridi 2012
Floridi, Luciano 'The informational nature of personal identity' in *Minds & Machines* 2012.

Foucault 1988
Foucault, Michel *Technologies of the Self. A Seminar with Michel Foucault*. L. H. Martin, H. Gutman, P. H. Hutton (ed.) Massachusetts: University of Massachusetts Press 1988.

Freire 2010
Freire, Gustavo Henrique de Araujo (ed.) *Ética da informação. Conceitos – Abordagens – Aplicações* João Pessoa 2010. Available at http://ru.ffyl.unam.mx:8080/bitstream/10391/1328/1/teaching%20information%20ethics.pdf

Fuchs 2009
Fuchs, T. *Das Gehirn – ein Beziehungsorgan. Eine phänomenologisch-ökologische Konzeption* 2nd ed. Stuttgart: Kohlhammer 2009.

Ganascia 2009
Ganascia, J.-G. 'The Great Catopticon' in *Proceedings of the 8th International Conference of Computer Ethics Philosophical Enquiry (CEPE)* 26-28 June 2009, Corfu, Greece.

Gavison 1980
Gavison, Ruth 'Privacy and the Limits of the Law' in *Yale Law Journal* No. 89 1980 pp. 421-471.

Giracca 2008
Giracca, Anabella 'El acceso a la información en países culturalmente diversos' in *Primera conferencia regional, latinoamericana y del Caribe sobre infoética en el ciberespacio* Santo Domingo, Ed. Funglode 2008 pp. 79-87. Available at http://www.redciberetica.org/documentos?func=startdown&id=%201

Gonzalbo 2004
Gonzalbo, Pilar (ed.) *Historia de la vida cotidiana en México* México: FCE- Colmex 2004ff.

Greenleaf 2012
Greenleaf, Graham 'The influence of European data privacy standards outside Europe: Implications for globalisation of Convention 108?' *Research Paper Series* No. 2012/12.

Habermas 1962/1990
Habermas, Jürgen *Strukturwandel der Öffentlichkeit* Frankfurt/M.: Suhrkamp 1962/1990).

Habermas 1995
Habermas, Jürgen 'Kants Idee des Ewigen Friedens. Aus dem historischen Abstand von 200 Jahren' in *Information Philosophie* 5, Dezember 1995 pp. 5-19. 1995.

Hauptman & Soffer 2011
Hauptman, Aharon Yair Sharan & Tal Soffer 'Privacy Perception in the ICT era and beyond' in von Schomberg 2011.

Hegel RPh. 1970
Hegel, G.W.F. Rechtsphilosophie in *Werke* Bd. 7 Frankfurt/M.: Suhrkamp 1970.

Heidegger EiM 1953
Heidegger, Martin *Einführung in die Metaphysik* Tübingen: Niemeyer 1953.

Heidegger GA24 1975
Heidegger, Martin *Die Grundprobleme der Phänomenologie* Marburger Vorlesung SS 1927 *Gesamtausgabe* Band 24 (GA24) ed. F-W. v. Herrmann, Frankfurt/M.: Klostermann 1975 English translation: *The Basic Problems of Phenomenology* Indiana U.P. 1982.

Heidegger SZ 1927
Heidegger, Martin *Sein und Zeit* Tübingen: Niemeyer 1927, 15th ed. 1984.

Heidegger ZS 1969
Heidegger, Martin 'Zeit und Sein' in *Zur Sache des Denkens* Tübingen: Niemeyer 1969.

Hobbes Vol. VII 1928
Hobbes, Thomas *Elements of Law* in *Works* Vol. VII. Cambridge U.P. 1928.

Hobbes 1651/1997
Hobbes, Thomas *Leviathan* (1651) eds. Richard E. Flathman and David Johnston, Norton, New York/London 1997.

Höffe 1997
Höffe, Ottfried, entry on Gerechtigkeit in *Lexikon der Ethik* Munich: Beck 1997.

Höffe 1989
Höffe, Ottfried 'Rechtsordnung als gerechter Tausch' in *Universitas* 1/ 1989 pp. 11-17.

Hofmann 1984
Hofmann, H. Eintrag 'Öffentlich/privat' in Joachim Ritter und Karlfried Gründer (eds.): *Historisches Wörterbuch der Philosophie* Darmstadt: Wiss. Buchgesell. 1984 Bd. 6, Sp. 1131-1134.

Hongladarom 2007
Hongladarom, Soraj 'Analysis and Justification of Privacy from a Buddhist Perspective' in Hongladarom and Ess 2007 pp. 108-122.

Hongladarom & Ess 2007
Hongladarom, Soraj and Charles Ess (eds.) *Information Technology Ethics. Cultural Perspectives* Hershey PA, Idea Group Reference 2007.

Huxley 1932
Huxley, Aldous *Brave New World* 1932, Folio Society edition, London 1971.

Jullien 1995
Jullien, François *Le détour et l'accès. Stratégies du sens en Chine, en Grèce* Paris, Presses Universitaires de France 1995.

Jullien 2005
Jullien, François *Nourrir sa vie. À l'écart du bonheur* Paris, Seuil 2005 (Engl. transl. by A. Goldhammer *Vital Nourishment. Depart from happiness* The MIT Press 2007).

Jullien 2008
Jullien, François *De l'universel, de l'uniforme, du commun et du dialogue entres les cultures*. Paris, Fayard 2008.

Kant 1781/1787
Kant *Kritik der reinen Vernunft* 1781/1787 *Werke* Bd. 2 Darmstadt, Wissenschaftliche Buchgesellschaft 1983.

Kant 1974
Kant, Immanuel 'Grundlegung zur Metaphysik der Sitten' in *Kritik der praktischen Vernunft* Frankfurt am Main, Suhrkamp 1974.

Kant 1974a
Kant, Immanuel *Kritik der praktischen Vernunft* Frankfurt am Main, Suhrkamp 1974a.

Kant 1975
Kant, Immanuel 'Beantwortung der Frage: Was ist Aufklärung?' in *Schriften zur Anthropologie, Geschichtsphilosophie, Politik und Pädagogik* Zweiter Teil, Darmstadt, Wissenschaftliche Buchgesellschaft 1975.

Kant 1975a
Kant, Immanuel 'Was heißt: sich im Denken orientieren?' in *Schriften zur Metaphysik und Logik* Darmstadt: Wissenschaftliche Buchgesellschaft 1975a.

Kant 1977
Kant, Immanuel *Die Metaphysik der Sitten: Metaphysische Anfangsgründe der Tugendlehre* Frankfurt am Main: Suhrkamp 1977.

Kant 1983
Kant, Immanuel 'Was ist der Mensch?' *Logik* in *Werke* Band III Darmstadt: Wissenschaftliche Buchgesellschaft 1983.

Kimura 1972
Kimura, Bin *Hito to hito to no aida* Tokyo, 1972 (German transl. E. Weinmayr *Zwischen Mensch und Mensch. Strukturen japanischer Subjektivität* Darmstadt, Wissenschaftliche Buchgesellschaft 1995).

Kitiyadisai 2005
Kitiyadisai, Krisana 'Privacy rights and protection: foreign values in modern Thai context' in *Ethics and Information Technology* Vol. 7 2005 pp. 17-26.

Kleve & de Mulder 2008
Kleve, Pieter & de Mulder, Richard 'Privacy protection and the right to information. In search of a new balance' in *Computer Law & Security Report* 24 (3) 2008 pp. 223–32.

Kranenburg 2008
Kranenburg, Rob van *The Internet of Things: A critique of ambient technology and the all-seeing network of RFID* Institute of Network Cultures, Amsterdam 2008. Available at http://www.networkcultures.org/networknotebooks accessed October 2011

Kusch 1962/1975
Kusch, Rodolfo *América profunda*. Buenos Aires: Hachette 1962, 2nd ed. 1975.

Kusch 1976/2010
Kusch, Rodolfo *Indigenous and Popular Thinking in América* Durham and London, Duke U.P: 2010 (orig. *Pensamiento indígena y pensamiento popular en América* 1976).

Laimer & Nagel 2012
Laimer, Simon & Nagel, Daniel *'Rügeversäumnis und Beweislastverteilung im UN-Kaufrecht' IHR* 2012 pp. 42-44.

Legge et al. 1992
The Chinese/English Four Books translated by James Legge, revised and annotated by Liu Zhongde & Luo Zhiye, Changsha Hunan Press 1992.

Leibniz 2003
Leibniz, Gottfried Wilhelm 'Das Leib-Seele-Pentagon und die moralische Sphäre des Verstandes' in *Frühe Schriften zum Naturrecht* (ed.) Hubertus Busche, Meiner, Hamburg 2003.

Locke 1690
Locke, John *An Essay Concerning Human Understanding* various editions, original edition 1690.

Locke 1965
Locke, John *Two Treatises of Government* with an introduction by Peter Laslett, Mentor Books, New York 1965.

Löwith 1928/1981
Löwith, Karl *Das Individuum in der Rolle des Mitmenschen* (1928) reprinted in *Sämtliche Schriften* Bd. 1 K. Stichweh (ed.) Metzler, Stuttgart 1981.

Lü 2005
Lü, Yao-huai 'Privacy and data privacy in contemporary China' in *Ethics and Information Technology* Vol. 7 2005 pp. 7-15.

Lü 2007
Lü, Yao-huai 'Globalization and Information Ethics' in Capurro et al. 2007 pp. 69-73.

Mannuzza 2008
Mannuzza, Francisco 'Las culturas indígenas venezolanas en el ciberespacio: refléxiones éticas' in *Primera conferencia regional, latinoamericana y del Caribe sobre infoética en el ciberespacio* Santo Domingo, Ed. Funglode 2008 pp. 225-234. Available at http://www.redciberetica.org/documentos?func=startdown&id=%201

Marx 1974
Marx, Karl *Grundrisse der Kritik der Politischen Ökonomie* Dietz, Ost-Berlin 1974.

Marx 1962
Marx, Karl *Das Kapital* in *Marx Engels Werke* Bde. 23, 24, 25 Dietz, Ost-Berlin 1962 Abbreviated MEW.

McDougall & Hansson 2002
McDougall, Bonnie S. & Hansson, Anders *Chinese Concepts of Privacy* Leiden, Brill 2002.

MISTICA 2002
MISTICA Virtual Community *Working the Internet with a social vision* 2002. Available at http://www.funredes.org/mistica/english/cyberlibrary/thematic/eng_doc_olist2.html

Mizutani et al. 2004
Mizutani, Masashiko, James Dorsey & James A. Moor 'The Internet and Japanese conception of privacy' in *Ethics and Information Technology* Vol. 6 2004 pp. 121-128.

Moor 1997
Moor, James H. 'Towards a theory of privacy in the information age' in *Computers and Society* 27(3) 1997 pp. 27-32.

Moor 2004
Moor, James H. 'Reason, relativity, and responsibility in computer ethics' in Spinello R.A. and Tavani H.T. (eds.) *Readings in CyberEthics* 2nd ed. Sudbury MA: Jones & Bartlett 2004 pp. 40-54.

Nagel 1988
Nagel, Thomas 'Concealment and Exposure' in *Philosophy and Public Affairs* 1988 No. 27. Available at http://www.nyu.edu/gsas/dept/philo/faculty/nagel/papers/exposure.html

Nagel 2011a
Nagel, Daniel 'IPv 6 und Datenschutz: Personalisiertes Surfen mit Gefahren für die Privatsphäre' LTO 2011.

Nagel 2011b
Nagel, Daniel 'Beware of the Virtual Doll ISPs and the Protection of Personal Data of Minors' in *Philosophy & Technology* 2011 pp. 411-418 (DOI) 10.1007/s13347-011-0034-7.

Nagenborg 2009
Nagenborg, Michael 'Designing Spheres of Informational Justice' in *Ethics and Information Technology* Vol. 11, No. 3, 2009 pp. 175-179.

Nagenborg 2005
Nagenborg, Michael *Das Private unter den Rahmenbedingungen der IuK-Technologie. Ein Beitrag zur Informationsethik* Wiesbaden: VS Verlag 2005.

Nakada 2007
Nakada, Makoto 'The Internet within Seken as an old and indigenous world of meanings in Japan' in Capurro, Frühbauer & Hausmanninger (eds.) 2007 pp. 177-203.

Nakada & Takanori 2005
Nakada, Makoto & Takanori Tamura 'Japanese conceptions of privacy: An intercultural perspective' in *Ethics and Information Technology* Vol. 7 2005 pp. 27-36.

Nissenbaum 1998
Nissenbaum, Helen 'Protecting Privacy in an Information Age: The Problem of Privacy in Public' *Law and Philosophy* No. 17 1998 pp. 559-596. Online: http://www.nyu.edu/projects/nissenbaum/papers/privacy.pdf accessed November 2011.

Nissenbaum 2004
Nissenbaum, Helen 'Privacy as contextual integrity' in *Washington Law Review* 79(1) 2004 pp. 119-157.

Nissenbaum 2010
Nissenbaum, Helen *Privacy in Context: Technology, Policy, and the Integrity of Social Life* Stanford U. P. 2010.

Novais & Moritz Schwarcz 1997
Novais, Fernando A. & Lilia Moritz Schwarcz *Historia da vida privada no Brasil* São Paulo: Companhia Das Letras 1997ff.

Olinger et al. 2005
Olinger, H.N., Johannes Britz & M.S. Olivier 'Western privacy and ubuntu: influences in the forthcoming data privacy bill' in Philip Brey, Frances Grodzinsky, Lucas Introna (eds) *Ethics and New Information Technology* Enschede, The Netherlands, CEPE 2005 pp. 291-306.

Orito 2011
Orito, Yohko, Eunjin Kim, Yasunori Fukuta and Kiyoshi Murata 'Online Privacy and Culture: A Comparative Study between Japan and Korea' in *ETHICOMP* Sheffield Hallan University 2011. Available at http://www.ccsr.cse.dmu.ac.uk/conferences/ethicomp/ethicomp2011/abstracts/ethicomp2011_33.php

Penrose R. 1999
Penrose R. *The Emperor's New Mind: Concerning Computers, Minds and The Laws of Physics* 2nd ed. Oxford U.P., Oxford 1999.

Pfeiffer 2008
Pfeiffer, María Luisa 'Derecho a la privacidad. Protección de los datos sensibles' in *Revista Colombiana de Bioética* Vol. 3 No. 1 2008, pp. 11-36. Available at http://redalyc.uaemex.mx/src/inicio/ForazarDescargaArchivo.jsp?cvRev=1892&cvArt=189217248002&nombre=Derecho%20a%20la%20privacidad.%20Protecci%F3n%20de%20los%20datos%20sensibles

Pimienta 2007
Pimienta, Daniel 'At the Boundaries of Ethics and Cultures: Virtual Communities as an Open Ended Process Carrying the Will for Social Change (the MISTICA experience)' in Capurro et al. 2007 pp. 205-228.

Ramasota 2007
Ramasota, Pirongrong 'Information Privacy in a Surveillance State: A Perspective from Tahiland' in Hongladarom & Ess 2007 pp. 124-137.

Ramose 2002
Ramose, Mogobe B. 'Globalization and *ubuntu*' in Peter H. Coetzee & Abraham P. J. Roux (eds.) *Philosophy from Africa. A text with readings* Oxford U.P. 2nd ed. 2002 pp. 626-650.

Rawls 1971
Rawls, John *A Theory of Justice* The Belknap Press of Harvard University Press first edition 1971.

Regan 1995
Regan, P.M. *Legislating Privacy: Technology, Social Values, and Public Policy* Chapel Hill NC: North Carolina U.P. 1995.

Ricardo 1821/1996
Ricardo, David *Principles of Political Economy and Taxation* (1821) New York: Prometheus Books 1996.

Rössler 2004
Rössler, Beate *The Value of Privacy* transl. R.D.V. Glasgow, Cambridge: Polity Press 2005.

Röttgers 2011
Röttgers, Kurt 'Wirtschaftsethik, Wirtschaftsmoral und die Aufgaben der Wirtschaftsphilosophie' in Hubertus Busche (ed.) *Philosophische Aspekte der Ökonomie* Würzburg 2011 pp. 39-54.

Roth 2003
Roth, G. *Aus Sicht des Gehirns* Suhrkamp, Frankfurt 2003.

Sagredo & Gazmuri 2005
Sagredo, Rafael & Cristián Gazmuri (eds.) *Historia de la vida privada en Chile* Santiago: Taurus-Aguilar Chilena de Ediciones 2005.

Scheule et al. 2004
Scheule, Rupert M., Rafael Capurro & Thomas Hausmanninger (eds.) *Vernetzt gespalten. Der Digital Divide in ethischer Perspektive* ICIE Schriftenreihe Bd. 3 Munich, Fink 2004.

Schomberg 2011
Schomberg, René von (ed.) *Towards Responsible Research and Innovation in the Information and Communication Technologies and Security Technologies Fields* A Report from the European Commission Services, Luxembourg Publications Office of the European Union 2011.

Sen & Kliksberg 2005
Sen, Amartya Kumar & Bernardo Kliksberg (eds.) *La agenda ética pendiente en América Latina* Buenos Aires, Fondo de cultura económica 2005.

Shannon 1948
Shannon, Claude E. 'A Mathematical Theory of Communication' in *The Bell System Technical Journal* Vol. 27, July, October, 1948 pp. 379–423, 623–656.

Shannon & Weaver 1949/1998
Shannon, Claude E. and Weaver, Warren *The Mathematical Theory of Communication* Illinois U.P. 1949, 1998.

Singer 2004
Singer, W. 'Selbsterfahrung und neurobiologische Fremdbeschreibung' *Deutsche Zeitschrift für Philosophie* 2004, 4 pp. 175-190.

Smith 1759/2000
Smith, Adam *The Theory of Moral Sentiments* (1759) New York: Prometheus Books 2000.

Smith 1776/2000
Smith, Adam *The Wealth of Nations* (1776) edited with notes, marginal summary and enlarged index by Edwin Cannan, New York: The Modern Library 2000.

Swanson 1992
Swanson, Judith A. *The Public and the Private in Aristotle's Political Philosophy* Ithaca, London: Cornell U.P. 1992.

Tavani 2008
Tavani, Herman T. 'Informational Privacy: Concepts, Theories, and Controversies' in Kenneth E. Himma & Herman T. Tavani (eds.) *The Handbook of Information and Computer Ethics* Hoboken NJ: Wiley 2008 pp. 131-164.

Tavani & Moor 2001
Tavani, Herman T. & Moor, James. H. 'Privacy Protection, Control of Information, and Privacy-Enhancing Technologies' in Richard D. Spinello & Herman T. Tavani (eds.) *Readings in CyberEthics* Boston: Jones and Bartlett 2001 pp. 378-391.

Theunissen 1977
Theunissen, Michael *Der Andere: Studien zur Sozialontologie der Gegenwart* 2nd ed. Berlin/New York: W. de Gruyter 1977.

Turing 1936
Turing, Alan M. 'On Computable Numbers, with an Application to the Entscheidungsproblem' in *Proc. Lond. Math. Soc.* (2) 42 1936 pp. 230-265.

Turner 1967
Turner, Victor *The Forest of Symbols: Aspects of Ndembu Ritual* Cornell U. P. 1967.

Turner 1974
Turner, Victor *Dramas, Fields, and Metaphors: Symbolic Action in Human Society* Cornell U. P. 1974.

Van den Hoven 2001
Van den Hoven, Jeroen 'Privacy and the Varieties of Informtional Wrongdoing' in Richard A. Spinello and Herman T. Tavani (eds.) *Readings in CyberEthics* Jones and Bartlett, Sudbury MA 2001 pp. 230-242.

Von Barloewen 1992
Von Barloewen, Constantin *Kulturgeschichte und Modernität Lateinamerikas* Munich, Matthes & Seitz 1992.

Vedder 2004
Vedder, A.H. 'KDD, privacy, individuality, and fairness' in Spinello R.A. & Tavani H.T. (eds.) *Readings in CyberEthics* 2nd ed. Jones and Bartlett, Sudbury MA 2004 pp. 462-470.

Walzer 1983
Walzer, Michael *Spheres of Justice: A Defense of Pluralism and Equality* Basic Books, New York 1983.

Westin 1967/1970
Westin, Alan F. *Privacy and Freedom* New York: Atheneum,1967, London: The Bodley Head 1970

Weyl 1918
Weyl, Hermann *Das Kontinuum* Leipzig: Veit & Co. 1918.

Wiener 1948/1961
Wiener, Norbert *Cybernetics, or Control and Communication in the Animal and the Machine* MIT Press 1948, 1961.

Winograd & Flores 1986
Winograd, Terry & Flores, Fernando *Understanding Computers and Cognition. A new foundation for design* Ablex 1986.

Wohlfart 2002
Wohlfart, Günter 'Alte Geschichten zum wuwei' in Rolf Elberfeld & Günter Wohlfahrt (eds.): *Komparative Ethik. Das gute Leben zwischen den Kulturen* Cologne, Edition Chora 2002 pp. 97-106.

Woolf 1928/2007
Woolf, Virginia *Orlando: A Biography* 1928 *Selected Works* London: Wordsworth Editions 2007.

Woolf 1931/2007
Woolf, Virginia *The Waves* 1931 *Selected Works* London: Wordsworth Editions 2007.

Woolf 1938/2007
Woolf, Virginia *Three Guineas* 1938 *Selected Works* London: Wordsworth Editions 2007.

3 VERTRAUENSINFRASTRUKTUR UND PRIVATHEIT ALS ÖKONOMISCHE FRAGESTELLUNG

GÜNTER MÜLLER, CHRISTIAN FLENDER, MARTIN PETERS

ZUSAMMENFASSUNG

Nicht nur die gesetzliche Regulierung, sondern auch die Individualisierung durch das Internet weist der Privatheit sowohl eine einzel- als auch gesamtwirtschaftliche Rolle zu. Dabei wird Privatheit aus Anbietersicht oft als Kostenfaktor gesehen, dem wenige Erträge gegenüberstehen. Aus Nachfragesicht lässt die geringe Akzeptanz von Privacy Enhancing Technology (PET) darauf schließen, dass Privatheit zu einem Auslaufmodell werden könnte. Der Beitrag zeigt, dass durch die Nutzung von persönlichen Daten wirtschaftliche Werte geschaffen werden, deren Grundlage am wirkungsvollsten durch die Kontrolle der Verwendung und nicht durch das Verbot zur Sammlung geschützt werden kann. Die Analyse von empirischen Szenarien des E-Commerce und sozialer Netzwerke zeigt, dass Privatheit sowohl die Einzelentscheidungen des Nutzers als auch des Anbieters verändern kann, und so für alle datenzentrischen Dienste zu einem kritischen Faktor für die Nachhaltigkeit des Geschäftsmodells werden könnte. Das Privacy Paradox und die Datenverwertung führen zu vier Thesen. Diese veranschaulichen die Anforderungen an PET in Bezug auf das Verhindern von Informationsdefiziten aus wirtschaftlicher Sicht und empfehlen, diese durch Mechanismen zur Erhöhung der Transparenz zu ergänzen.

ABSTRACT

For individual economic activities as well as the economy at large, the role of privacy is determined not only by regulation but also by personalization enabled by the internet. First and foremost, from the point of view of suppliers, privacy incurs costs and no benefits. From a consumer standpoint, the low acceptance of Privacy Enhancing Technologies (PET) suggests that privacy will be an obsolescent model in the near future. The chapter at hand demonstrates, however, that the generated economic value by using personal data can best be protected by control of the usage of data and not solely by its collection. Based upon analyses of empirical usage scenarios in e-commerce and data-centric services like social networks, it is argued that a lack of privacy bears the potential to change both decisions of consumers and service providers and has become a critical factor of sustainability of many internet-based business models. In relation to the use of such services, the privacy paradox and data usage raises four theses which highlight the requirements needed within current PET to avoid information deficits and the need for mechanisms to enable transparency.

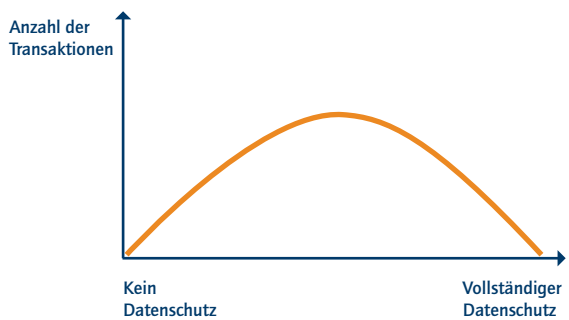
3.1 EINFÜHRUNG

Privatheit ist im Deutschen ein Kunstwort, dessen Bedeutung, neben dem üblichen Begriff Privatsphäre, das amerikanische Privacy umfassen soll. Hierbei handelt es sich um eine ethische oder soziologische Kategorie, die in der Jurisprudenz durch die informationelle Selbstbestimmung oder in den Wirtschaftswissenschaften als Eigenschaft von Produkten eine wichtige Rolle spielt. In ökonomischer Hinsicht ist Privatheit dann von Relevanz, wenn sie auf das Marktverhalten Einfluss nimmt, zum Beispiel wenn im Vertrauen auf Erfüllung eines Privatheitsversprechens ein Kauf getätigt oder abgelehnt wird. Aus einzelwirtschaftlicher Sicht wird Privatheit daher als eine Eigenschaft von Produkten definiert, die gleichberechtigt neben anderen Eigenschaften, wie zum Beispiel den verwendeten Materialien, die Wertbestimmung beeinflusst. Eine davon abweichende Auffassung zur Betrachtung von Privatheit im Wirtschaftlichen ordnet Eigenschaften nicht dem Produkt selbst zu, sondern setzt sie in Relation zu Präferenzen der Kunden. Beispielsweise kaufen Kunden mit der Präferenz einer gerechten Arbeitswelt Fair-Trade Kaffee, weil damit ein Signal auf die Herstellungsweise gegeben wird. Aber auch in diesem Fall ist letztlich Privatheit mit der Spezifikation des Produktes verbunden, das zum Tausch angeboten wird.

In gesamtwirtschaftlicher Sicht stellt sich die Sache anders dar: Hier ist Privatheit die Fähigkeit, die Verteilung von Informationen zu beeinflussen. Eine ungleiche Verteilung von Zugang und Verfügbarkeit von Informationen führt zu Kaufentscheidungen, die im Sinne der Volkswirtschaft zu Ineffizienzen bei der Allokation von Ressourcen führt und daher den Wohlstand potenziell negativ beeinflusst. Eine für die Gesamtwirtschaft wirksame Vertrauensinfrastruktur sollte Informationsungleichgewichte vermeiden. Diese ist dann erreicht, wenn sich alle Markteilnehmer entweder gesetzlich gezwungen oder freiwillig an Normen und Regeln halten, die den Zugang und Umgang mit Daten und Informationen betreffen. Wirtschaftliches Handeln ohne Datenaustausch ist unvorstellbar. Beim Überlassen von Daten an Dritte besteht jedoch die Gefahr des Missbrauches und damit auch die Gefahr eines Vertrauensbruchs. Ferner besteht die Möglichkeit, Daten zu sammeln, daraus Profile abzuleiten und somit das Kaufverhalten eines Kunden in der Form zu beeinflussen, dass dieser ohne den Datenvorteil des Marktpartners zu anderen Entscheidungen gekommen wäre. Die Kontrolle und Durchsetzung des Schutzes von Informationen wird sehr häufig an sogenannte vertrauenswürdige Dritte übertragen. Prinzipiell werden damit die Risiken der Fehlallokation eingeschränkt und es wird zusammen mit Techniken zur Anonymisierung und Pseudonymisierung die Profilbildung eingeschränkt.

Insgesamt ist davon auszugehen, dass eine Vertrauensinfrastruktur die Wirtschaft nach der in Abbildung 1 gekennzeichneten Form beeinflusst. Während die Ordinate die Zahl der Transaktionen und damit eine Voraussetzung für gesellschaftlichen Wohlstand kennzeichnet, beschreibt die Abszisse den Grad an Privatheit. Die Kurve unterliegt der Annahme – empirische Untersuchungen zum Verhältnis von Privatheit und wirtschaftlicher Dynamik fehlen bislang –, dass kein Datenschutz ebenso wie vollständiger Datenschutz die wirtschaftliche Interaktion zum Erliegen bringen würde. Beides ist nicht wünschenswert und stellt daher die zu vermeidenden Extrempunkte einer Vertrauensinfrastruktur für das Internet dar.

Abbildung 1: Datenschutz und wirtschaftliche Interaktion



Die wichtigsten und wirtschaftlich relevantesten Szenarien sind der E-Commerce und die sozialen Dienste. Während sich der E-Commerce auf die Nutzung des zusätzlichen elektronischen Kanals zwischen Kunden und Anbietern konzentriert und beachtliche Fortschritte in der gesamtwirtschaftlichen Effizienz erzielt hat, sind die sozialen Dienste durch die Beteiligung der Marktteilnehmer an der Wertschöpfung gekennzeichnet. Die Individualisierung der Beziehung von Nachfrager und Anbieter durch das Internet verlangt von Anbietern die Kenntnis persönlicher Daten der Kunden, um am Markt bestehen zu können. Wertschöpfungsketten werden zunehmend kooperativ unter Einschluss der Kunden oder verteilt durch Koordination ausführbar. Zur Koordination sind auch persönliche Daten notwendig, deren Sammlung und Auswertung gegenwärtig selbst einer Spezialisierung und dem wirtschaftlichen Wettbewerb unterliegen. Daher werden derzeit zunehmend Informationen mit Aussicht auf Ertrag gesammelt, verkauft und verwertet. Der Erwerb und Umgang mit Daten kommt dabei in verschiedenen Varianten vor und wird zusammenfassend als „Management der Kundenbeziehungen" (Customer Relationship Management (CRM)) bezeichnet. In Bezug auf den Umfang einer Transaktion kann prinzipiell zwischen einer begrenzten und einer erweiterten Sichtweise unterschieden werden. Bei Rabattkarten ist die Datensammlung mit der Transaktion verbunden und der Benutzer hat eine erweiterte Kenntnis über den Zweck der mit der eigentlichen Transaktion verbundenen Handlung. Bei vielen Web 2.0-Diensten hält sich die Kenntnis des Nutzers in Grenzen; bestenfalls ist er über die Datensammlung informiert, die spätere Nutzung und deren Rückwirkung kennt er jedoch nicht vollständig.

CRM geschieht aktuell dann besonders effizient, wenn zwischen Kunde und Anbieter ein Intermediär eingeschaltet wird, der die Datensammlung, Auswertung und die Plattformbereitstellung übernimmt. Hierbei können zwei wesentliche Varianten unterschieden werden: Entweder erwerben Organisationen persönliche Daten durch Ankauf oder sie bieten einen Teil ihrer attraktiven Dienste als Gegenleistung für die Überlassung persönlicher Daten an. Aus gesamtwirtschaftlicher Sicht besteht nun die Herausforderung einer Vertrauensinfrastruktur, dafür zu sorgen, dass es nicht systematisch zu Ungleichverteilungen von Informationen kommt, die zu Ineffizienzen führen.

Aus einzelwirtschaftlicher Sicht ist zu klären, ob und welche Privatheitsforderungen Geschäftsmodelle ermöglichen, die in ihrem Nettoeffekt zur individuellen und gesamtwirtschaftlichen Wohlfahrt beitragen. Dazu wäre es hilfreich, wenn für die Privatheit ein wirtschaftlicher Gegenwert ermittelt werden könnte, der angibt, was Privatheit dem Einzelnen wert ist. Aus Anbietersicht bildet dann die Erwartung an die Einhaltung – zum Beispiel des Privatheitsversprechens – einen Teil des Entgeltes, den der Nachfrager für ein Produkt zu zahlen bereit ist. Diese Beziehung von Privatheit und wirtschaftlicher Aktivität konnte in Einzelfällen nachgewiesen werden und reflektiert den in Abbildung 1 gezeigten Verlauf. In der Realität sind jedoch die Fälle in der Mehrheit, bei denen eine Beziehung zwischen Privatheit und wirtschaftlichem Fortschritt nicht nachgewiesen werden konnte. Dies ist beim gesetzlichen Datenschutz der Fall, der davon ausgeht, dass der Schutz für die wirtschaftliche Entwicklung einen positiven Beitrag leistet und der daher für spezielle Bedingungen die Privatheit reguliert. So verlangt das Bundesdatenschutzgesetz, aber auch die Richtlinien der OECD, dass Daten nur für einen bestimmten Zweck erhoben und falsche Daten korrigiert werden müssen. Für alle interessierten Marktteilnehmer muss also Transparenz in Bezug auf die Datensammlungen bestehen.

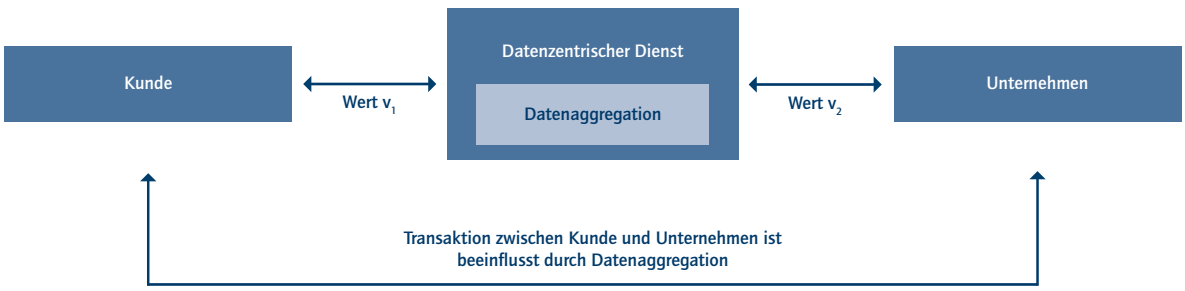
Bestimmt durch den Trend zur Individualisierung der Beziehungen zwischen Anbieter zum Kunden, gerät nun die transaktionsaktionsspezifische Interpretation des Datenschutzes in die Kritik. Moderne Verfahren der Business Intelligence und flexible, kundenorientierte Managementtechniken zur nachhaltigen Aufrechterhaltung der Kundenbeziehungen

sind auf persönliche Datenbestände angewiesen, die zunehmend gesammelt werden, ohne die Betroffenen zu informieren oder gar unmittelbar einem vorbestimmten Zweck zugeordnet zu werden. In diesem Falle bezahlt der Nachfrager für den Erwerb eines Produktes einen informationellen Preis, den er nicht abschätzen kann. Diese Datensammlungen können in späteren Transaktionen Grundlage für die Interaktion von Marktteilnehmern werden, deren Existenz und Bedeutung bei mangelnder Transparenz nur einer Seite bekannt zu sein brauchen. Es ist dann von einer verzögerten Wirkung der Daten in nachfolgenden Transaktionen auf die Kundenentscheidung auszugehen. Datensammlungen entstehen meist als Folge eines legalen und in seiner Struktur transparenten Geschäftsmodells. Die Dienste des Web 2.0, die nachfolgend als datenzentrische Dienste bezeichnet werden, sammeln persönliche Daten in der Weise, dass sie die meist kostenfreie Nutzung attraktiver Dienste gegen private Daten eintauschen. Durch die Einschaltung des Intermediärs „Datenzentrischer Dienst" ist eine Transaktion damit in zwei zusammenhängende Teiltransaktionen aufgespalten, die beim datenzentrischen Dienst zu Datenaggregation führt, die dieser wiederum seinen zahlenden Kunden, meist Unternehmen, in diversen Formen anbietet.

In Abbildung 2 ist die Struktur einer solchen zweiwertigen Transaktion dargestellt. In der Beziehung des Kunden – er ist ja der eigentliche Datenanbieter – zum Intermediär wird durch die Nutzung eines attraktiven Dienstes beim Kunden ein wirtschaftlicher Wert v1 erzeugt. Der Nutzen des Intermediärs liegt im Vertrieb der dabei anfallenden persönlichen Daten; hierfür muss er die Daten zuvor aufzeichnen. Der Nachfrager solcher Daten im zweiten Teil der Transaktion ist nur in sehr geringem Umfang der Intermediär. Vorrangiger Nachfrager ist ein dritter Datenkonsument oder Datennutzer. Die Beziehung Intermediär zum finalen Datenkonsumenten erzeugt den wirtschaftlichen Wert v2. Eine solche zweiwertige Transaktion ist dadurch gekennzeichnet, dass der Wert v2 erst durch das Geschäft v1 entstehen kann, also durch dieses bedingt ist. Ferner wirkt der Wert v2 meist nicht unmittelbar auf die von Kunden ausgelöste Transaktion, sondern beeinflusst erst verspätet oder verzögert für eine andere Transaktion das Kundenverhalten. Zur Verhandlung der neuen Transaktion können Daten eingesetzt werden, die dem Kunden nicht offenkundig sein müssen, die aber aus den Datenaggregationen der datenzentrischen Dienste abgleitet sind. Es gibt auch Erwartungshaltungen von Kunden, die einen unmittelbaren Effekt auf die aktuelle Transaktion haben können; so ist zum Beispiel die Verweigerung der Bekanntgabe der E-Mail-Adresse eine Folge der Kenntnis von v2. Man erwartet, dass diese Adressen zu Werbezwecken eingesetzt und zu Spam führen können.

Unabhängig davon, ob es sich nun um eine direkte beziehungsweise verzögerte Rückkopplung handelt, es kommt

Abbildung 2: Zweiwertige, verzögerte Transaktionen



zu Datenaggregationen, über deren exakten Inhalt der Kunde zurzeit und beim gegenwärtigen technischen Stand wenig weiß. Diese Datensammlungen legen Bedürfnisse der Kunden offen, die es denkbar werden lassen, dass Transaktionen zustande kommen, die ohne eine solche Kenntnis nicht stattgefunden hätten. Gleichzeitig ist es jedoch auch möglich, dass Transaktionen zwischen Datenanbieter und datenzentrischem Dienst nur deshalb stattfinden, weil der Datenanbieter falsche Annahmen bezüglich der Datenerhebung und Datenverwendung trifft. Durch die potenzielle Unwissenheit über die Nutzung von Datenaggregationen ist es denkbar, dass Kaufentscheidungen getroffen werden, ohne die Privatheit als Element des Tausches einzubeziehen. Solche möglichen Ungleichgewichte werden nachfolgend als Informationsdefizite bezeichnet. Die Auswirkungen und die Existenz von Informationsdefiziten sind wissenschaftlich bislang nicht nachgewiesen. Informationsdefizite sind ein Konstrukt, das die wirtschaftliche Relevanz von ausgewogener Informationsverteilung in Bezug auf die Anforderungen an eine Vertrauensinfrastruktur kenntlich macht. Die Zweiwertigkeit einer Transaktion und das Einschalten datenzentrischer Dienste als Vermittler verwehrt dem Primärnutzer von datenzentrischen Diensten dann jede Möglichkeit, den Wert seiner persönlichen Daten einzuschätzen, wenn keine Transparenz möglich ist. Der zyklische oder gar in Einzelfällen rekursive Charakter solcher Beziehungen verstärkt die Unfähigkeit zur Einschätzung über den in Wirklichkeit entrichteten Preis. Diese zyklische Verbundenheit der Transaktionen, ermöglicht über die Aggregationen von Daten und deren Einsatz, wird nachfolgend als Ursache für Informationsdefizite angesehen.

Informationsdefizite werden nicht aktiv erzeugt, sie entstehen als Beiprodukt von zweiwertigen Transaktionen durch das Nichtwissen über die Aggregation und die spätere Verwendung der Daten. Aus wirtschaftlicher Sicht ist die Forderung nach einer neuen Vertrauensinfrastruktur dadurch legitimiert, dass Informationsdefizite Entscheidungen ermöglichen, die auf unvollständiger beziehungsweise ungleicher Informationsbasis beruhen.

Bezogen auf den Kenntnisstand des Kunden zeigen zahlreiche empirische Untersuchungen, dass nicht von einer generellen Unkenntnis der Datenaggregation ausgegangen werden kann. Im Gegenteil – die überwiegende Mehrheit der Kunden ist sich bewusst, dass Daten gesammelt und aggregiert werden. Für den primären Datenanbieter überwiegen die mit dem Medium verbundenen Vorteile die Risiken, welche eine Nichtteilnahme bedeuten würde. Datenzentrische Dienste sind dann so relevant, dass ein Verzicht für den Einzelnen mit einer Aufgabe der Teilhabe zum Beispiel am öffentlichen und sozialen Leben oder der Nutzung wirtschaftlicher Vorteile verbunden wäre. So hat die Popularität der Web 2.0-Dienste inzwischen ein Maß erreicht, dass ein Aussteigen (opt-out) ohne erhebliche Nachteile für den Einzelnen unmöglich scheint.

Sofern ein Opt-out mehrheitlich unmöglich ist, besteht die Option zur Regulierung. Dem Prinzip der informationellen Selbstbestimmung folgt Europa. Das bedeutet, dass der oder die Einzelne selbst über die Verwendung der persönlichen Daten entscheiden soll. Hierzu müsste bei dem gegebenen Stand der datenzentrischen Dienste die Wirkung auf zukünftige Transaktionen mit anderen Partnern in einem anderen Kontext einschätzbar sein. Voraussetzung dafür aus technischer Sicht wäre eine Transparenz aller Aktivitäten der datenzentrischen Dienste in Bezug auf diese Person. Ein zur informationellen Selbstbestimmung alternativer Ansatz zur Privatheit ist die Rechtsnorm in Amerika, wo eine Unterscheidung in einen öffentlichen vs. privaten Raum getroffen wird, wobei Letzterer zu schützen ist. Im deutschen rechtsdogmatischen Denken gibt es den Begriff der Privatheit ebenso wenig, wie er gegenwärtig primär eine Kategorie des Wirtschaftlichen ist. Poscher bezeichnet daher das Recht auf informationelle Selbstbestimmung als abgeleitetes Recht.[360]

Unabhängig von der rechtlichen Situation ist die Akzeptanz von Privatheitsangeboten in den USA und Europa nahezu identisch. Eine Mehrheit der Konsumenten ist gleichzeitig

[360] Poscher 2012.

gegen die Sammlung und Verwertung von persönlichen Daten.[361] Für wirtschaftliche Zwecke und zur Aufrechterhaltung persönlicher Interaktion wird die Erhebung persönlicher Daten zur Realisierung des Wertes v1 jedoch in Kauf genommen. Der Einsatz nutzenstiftender Dienste senkt die Kosten zur Durchführung einer Transaktion und erhöht damit die individuelle Produktivität. Gesamtwirtschaftlich lassen die Untersuchungen am MIT für die Datenaggregation einen Beitrag zur Gesamtwohlfahrt vermuten, der höher eingeschätzt wird als die möglicherweise negativen Auswirkungen der Informationsdefizite. Im deutschen Wirtschaftsraum erheben alle Unternehmen, die ihre Geschäftsprozesse automatisiert haben, also ca. 65 Prozent der Unternehmen, persönliche Daten ihrer Kunden, ihrer Mitarbeiter und Geschäftspartner. Die positive Seite der Nutzung persönlicher Daten ist die in der Tat bessere Befriedigung von Kundenwünschen. Häufige Begründungen sind individualisierte Ansprachen der Kunden beziehungsweise die Individualisierung von Angeboten.[362]

Um zu verhindern, dass dabei entstehende Informationsdefizite zu Ineffizienzen beziehungsweise zu nachvertraglichem Andersverhalten führen, stehen für die Automatisierung der Vertrauensplattform prinzipiell zwei verschiedene Maßnahmen zur Verfügung:[363]

– *Signaling*: Die Anbieter geben von sich aus ein Signal, wie sie es mit der Privatheit von überlassenen Daten halten. Tatsächlich lässt sich empirisch nachweisen, dass viele Marktteilnehmer versuchen, durch Nutzung solcher Signale (zum Beispiel ein Gütesiegel), Informationsdefizite zu vermeiden. Dabei müssen die Kosten der Signalproduktion und -akzeptanz geringer sein als der Schaden ohne Signal. Die Anwendung von PET-Technologien ist ein solches Signal, das erhebliche Kosten bei manchmal umstrittenen Erträgen verursacht.
– *Screening*: Hierbei nimmt die uninformierte Marktseite Kosten auf sich, um durch Informationsbeschaffung ihre Informationsdefizite auszugleichen beziehungsweise zu kontrollieren, ob das *Signaling* der Wirklichkeit entspricht. Shop-Bots, Kataloge und das kollaborative Filtern zusammen mit dem von Google angeboten Dashboard sind Beispiele für Privatheitsmechanismen zur Erhöhung der Transparenz.

Fasst man zusammen, dann sind die Kosten, die für Mechanismen zum Signalling und Screening anfallen, nur dann aus wirtschaftlicher Sicht gerechtfertigt, wenn die Privatheit als Bestandteil der Produktbeschreibung entsprechend vom Kunden bewertet und honoriert wird. Privatheit als Produkteigenschaft unterscheidet sich dennoch von üblichen Produktbeschreibungen durch die zyklische oder verzögerte Wirkung. Informationsdefizite sind daher im Verbergen von relevanten Informationen durch den Informationsbesitzer zu sehen (information hiding). Ein ähnliches Verbergen läge auch vor, wenn der Kunde über die Materialzusammensetzung zum Beispiel eines Schmuckstückes, getäuscht würde. Signalling und Screening sind jedoch nur dann ein Differenzierungsmerkmal, wenn die Wahl zwischen verschiedenen Anbietern gegeben ist. Beim E-Commerce konnte bislang beobachtet werden, dass eine Tendenz zur Monopolbildung besteht.[364]

Natürliche Monopole sind gewissermaßen als die Informationsbesitzer zu betrachten, bei denen eine marktliche Regulierung nicht realisierbar erscheint. Aus ökonomischer Sicht sind Monopole dann als natürlich zu bezeichnen, wenn sie mit sinkenden Durchschnittskosten einhergehen. Ist dies der Fall, dann kann ein größeres Unternehmen die Nachfrage günstiger bedienen als kleinere Mitbewerber. Als Folge verlassen kleinere Unternehmen den Markt. Zudem entsteht eine hohe Barriere für einen Markteintritt von

361 CDT 2009.
362 Sackmann / Strüker 2005.
363 Shapiro / Varian 1999.
364 Müller / Eymann / Kreutzer 2003.

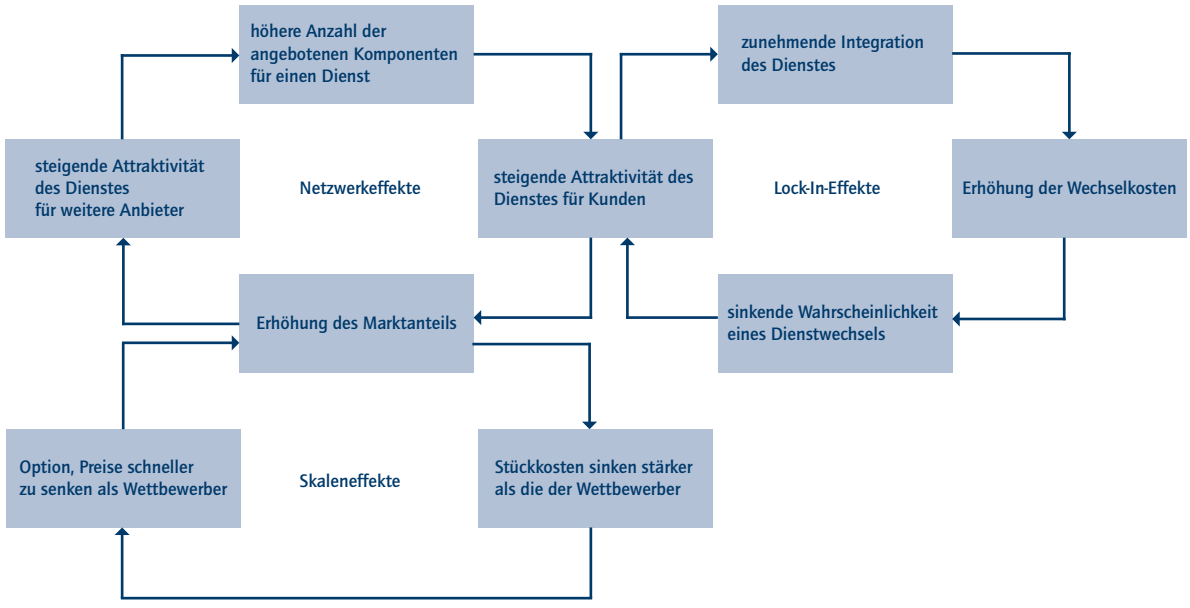
Mitbewerbern. Auf internetbasierten Märkten führen – neben sinkenden Stückkosten – oftmals weitere Faktoren zur Monopolsituation. Hier sind insbesondere die in Freiburg untersuchten positiven Rückkopplungseffekte zu nennen. Bei sozialen Netzwerken sind dies in erster Linie die Netzeffekte: Je mehr Nutzer ein soziales Netzwerk hat, desto attraktiver wird es für bestehende und potenzielle zukünftige Anwender. Zudem steigen die Wechselkosten, je länger ein soziales Netzwerk bereits genutzt wurde. Da es schwer möglich ist, veröffentlichte Inhalte in andere Netzwerke zu transferieren, verliert der Teilnehmer auch leicht einen wichtigen Teil seines sozialen Umfeldes. Abbildung 3 stellt dies und weitere Skaleneffekte sowohl für E-Commerce als auch für soziale Netze dar.

Eine neue Vertrauensinfrastruktur ist nur dann notwendig, wenn die alte Vertrauensinfrastruktur nicht mehr ausreicht, um wirtschaftliche Wohlfahrt und die Freiheit für einzelwirtschaftliches Handeln im Interesse aller Marktteilnehmer zu gewährleisten. Dabei verändert sich nicht nur die relative Position der Marktteilnehmer, sondern auch die Beiträge, die zum volkswirtschaftlichen Gesamtwohl erbracht werden können.

3.2 FAKTEN UND INFERENZEN: TRIEBKRÄFTE DER INTERNETÖKONOMIE

Das wirtschaftliche Motiv zur Datensammlung ist in den Individualisierungstendenzen der Kunden zu sehen, auf die Unternehmen reagieren müssen, wollen sie konkurrenzfähig bleiben. Die Voraussetzungen dazu liefern unter anderem datenzentrische Dienste. Hierzu bedienen sie sich diverser Formen, die anhand ihrer geographischen Reichweite und durch ihre Allgemeingültigkeit unterscheidbar sind. Klassische Formen des „Customer Relationship Managements"

Abbildung 3: Positive Rückkopplungseffekte[365]



[365] Müller / Eymann / Kreutzer 2003.

sind nur auf die Kunden eines Unternehmens bezogen. Die Auslagerung – und damit die Professionalisierung der Datensammlung durch spezialisierte Dienste – machen Daten und Schlussfolgerungen (Inferenzen) beziehungsweise deren Verfügbarkeit zur Handelsware.

Die datenzentrischen Dienste sind die aktuell wirtschaftlich günstigste, effizienteste, genaueste und globalste Form zur Datensammlung. Sie sind aus wirtschaftlicher Sicht aktuell durch folgende Eigenschaften gekennzeichnet: Zunächst sind sie frei für jedermann zugänglich und scheinbar kostenlos nutzbar. Der Preis wird in Form persönlicher Daten entrichtet. Während bei Diensten des statischen Web 1.0 bereits persönliche Daten gesammelt wurden, sind es im Web 2.0 nicht nur die Daten, sondern die aktuell noch in den Anfängen steckenden Möglichkeiten zur Ableitung neuer Daten aus bestehenden Datensammlungen. Man leitet Schlussfolgerungen ab, sogenannte „Inferenzen". Die Fähigkeit zur Ableitung von Inferenzen ist seit langem Gegenstand wirtschaftsinformatischer Forschungen und wird unter dem Schlagwort des „Business Intelligence" zusammengefasst,[366] worunter prominent die Verfahren des „Web Mining" gehören.[367] Inferenzen sind damit eine kreative und originäre Leistung datenzentrischer Dienste. Sie nicht unmittelbar personenbezogen und werden daher auch nicht von Regulierungsmaßnahmen erfasst. Dennoch basieren sie auf personenbezogenen Daten. Es gehört zu den Mythen der Sicherheitsforschung,[368] dass es personenbezogene Daten sein müssen, die von Relevanz für die Wirtschaft seien. Statt der persönlichen Identifikation sind Unternehmen eher an statistischen Klassifizierungen interessiert, die zu Mustern des Konsumentenverhaltens beziehungsweise zur Klassenbildung führen. Muster sind im Gegensatz zu Profilen nicht einem Individuum zugeordnet. Privatheit – wie wir sie bislang verstehen – ist dann gefährdet, wenn einzelne Personen identifizierbar sind. Das Geschäft mit Daten erfordert aber nicht notwendigerweise persönliche Identifikation. Lediglich die Zuordnung zu Klassen muss mit einem hohen Genauigkeitsgrad möglich sein, wobei letztlich der Gesamteffekt zur Erreichung geschäftlicher Interessen und nicht die Genauigkeit der Identifikation entscheidet.

3.2.1 SAMMLUNG

Es gibt wenig öffentlich verfügbares Wissen, um das Vorhandensein oder die Auswirkungen von Informationsdefiziten abzuschätzen. Ausgehend von der in Freiburg im Jahr 2005 durchgeführten Umfrage mit dem Titel *Stille Revolution* im E-Commerce[369] wird die Entwicklung vom bloßen Datensammeln hin zur Bildung von Inferenzen als eine sich wirtschaftlich und logisch ergebende Erweiterung des Geschäftsmodells datenzentrischer Dienste skizziert. Im Zeitraum von 1998 bis 2005 wurde das Internet überwiegend zur Rationalisierung der „Old Economy" eingesetzt und hat nur am Rande zur Sammlung von persönlichen Daten geführt. Ableitungen von Inferenzen waren 2005 in deutschen Unternehmen unbekannt, während Kundendaten schon von Anfang an gesammelt wurden. Die Rationalisierung der „Old Economy" schuf jedoch neben einem günstigen Vertriebskanal auch die Möglichkeit, die Wertschöpfung zu verändern. Neue Koordinationsformen zur verteilten Bereitstellung von Diensten und Waren wurden verfügbar und werden seit 2005 auch zunehmend genutzt. Virtuelle Unternehmen setzen auf Kooperation, wobei der wirtschaftliche Fortschritt in der Erzielung von Skaleneffekten durch Ausnutzen der Spezialisierung liegt. Spezialisierung erfordert Koordination, die wiederum auf der Nutzung von Daten beruht. Die Sammlung dieser Daten und die rationelle Form der Wertschöpfung sind das Geschäftsmodell datenzentrischer Dienste. Der Zusammenhang zur Privatheit ist primär der Schutz und die Regulierung der Verfügung über Daten.

366 Chamoni / Gluchowski 1997.
367 Cooley / Mobasher / Srivastava 1997.
368 Müller 2011.
369 Sackmann / Strüker 2005.

Das europäische Prinzip der informationellen Selbstbestimmung ist trotz des ihr innewohnenden demokratischen Ansatzes in die Kritik geraten. Untersuchungen und die täglichen persönlichen Erfahrungen zeigen, dass die Selbstbestimmung auf eine allgemeine Zustimmung der Geschäftsbedingungen reduziert wird, welche bei Nichtakzeptanz eine Verweigerung der Dienstnutzung zur Folge hat. Anbieter erkennen darin ein gesetzgeberisch auferlegtes Hindernis, um zu neuen Geschäftsmodellen zu gelangen; Kunden sehen in diesem Verhalten aktuell keine Bedrohung. Umfragen zeigen übereinstimmend, dass die Nutzer datenzentrischer Dienste überwiegend eine neue Form der Privatheit zum Leitbild machen. Die Alternative, entweder auf das Recht zu verzichten oder den Dienst nicht in Anspruch zu nehmen,[370] wird zulasten der Privatheit entschieden. Für Anbieter sind datenzentrische Dienste des Web 2.0 sehr effiziente „Datensammler" und liefern zusammen mit den Verfahren der „Business Intelligence" weit bessere und vor allem billiger zu erhaltende Daten, als dies zum Beispiel die herkömmliche Marktforschung vermag. Privatheit wird daher oft als orthogonal zum Erlösmodell charakterisiert. Prinzipiell ist der Wert der Daten aus wirtschaftlicher Sicht jedoch unbestritten, sodass marktliche Regelungen in den aktuellen Diskussionen zur Privatheit zunehmend an Relevanz gewinnen. Die Voraussetzung hierfür könnte die Regelung der Eigentumsverhältnisse an Daten sein, wobei die Auswertung dann in Übereinstimmung mit den Datenanbietern erfolgen müsste. Erste Hinweise auf einen Konflikt zu diesem Thema liefern die unterschiedlichen Positionen zum „Opt-in" und „Opt-out", wie wir sie in Europa und den USA beobachten können. In Europa ist für Internetdienste ein explizites „Opt-in" notwendig. In den USA ist es umgekehrt.[371]

3.2.2 VERWENDUNG

Daten werden von datenzentrischen Diensten aus Gründen der nicht zweckbezogenen Dokumentation mit dem Ziel der späteren Auswertung für unbestimmte Zeit gesammelt. Dies widerspricht den Prinzipien des aktuellen Datenschutzes, wonach der Zweck der Datensammlung und auch die Zeitdauer der Speicherung bekannt sein muss sowie Möglichkeiten zur Korrektur. Wirtschaftlich relevant ist nicht die Datensammlung, sondern deren Verwendung. In technischer Hinsicht spielt dabei vor allem die Nutzungskontrolle eine zentrale Rolle. Eine solche Begriffsbildung bezieht sich auf die Verwendung von Daten, während der bisherige Datenschutz auf deren Erhebung abzielt. Die Nutzungskontrolle dient der Transparenz und umfasst alle Techniken, die unter dem „Screening" zusammengefasst werden könnten, womit die im „Signalling" angegebenen Privatheitsversprechen der Anbieter überprüft werden können.

Ordnungspolitisch ist die Nutzungskontrolle problematisch, da sie als ein Verstoß gegen das Prinzip des Schutzes von Eigentum gesehen werden könnte, verlangt sie doch Einblicke in die Prozesse des Dienstanbieters. Während es bei erhobenen Daten noch vorstellbar ist, Transparenz zu ermöglichen, ist dies bei Inferenzen nur schwer durchzusetzen. Woher soll man wissen, welche Lehren aus den gesammelten Daten gezogen wurden und wie diese in zyklischen Transaktionen verwendet werden. Ferner bleibt verborgen, welchen Nutzen Daten tatsächlich gestiftet haben. Nutzer kooperieren mit datenzentrischen Diensten, weil es billig und bequem ist. Die Veränderung der Verfügbarkeit von Daten kann sehr deutlich an der Entwicklung der Organisation des Computing gezeigt werden. Es ist offensichtlich, dass es sich um eine technisch-soziale Co-Evolution handelt, die zum jetzigen Zeitpunkt wohl auch noch nicht abgeschlossen ist. Mit räumlicher Begrenzung haben Datenzentren bis zur Mitte der 1990er Jahre des vorigen Jahrhunderts „Computing" angeboten. Durch das Internet, den PC und mobile Endgeräte wie Smartphones und vor allem durch die Verbilligung der Telekommunikation ist eine Enträumlichung eingetreten, die solche zentralen Formen durch mehr dezentrale Formen des Rechnens ersetzt. Während der einzelne PC lange Zeit

370 Wohlgemuth 2009.
371 Slobogin 2012.

die Grenze darstellte, erfolgt nun über nutzerfreundliche Zugangsgeräte die Verfügbarkeit von nahezu unbegrenzter Rechenleistung. Benutzerfreundliche Dienste jeder Art werden aus einer „Wolke" (Cloud Computing) abgerufen, alle Daten sind dezentral und – ohne dass man den wirklichen Speicherort zu kennen braucht – jederzeit abrufbar. Schutzziele haben sich mit den Formen des Computing geändert:

- **Schutzziel in Datenzentren: Vertraulichkeit**
- **Schutzziel im Internet: Identität**
- **Schutzziel für Cloud: Transparenz und Kontrolle**

Kryptographie ist die Disziplin, die Vertraulichkeit gewährleistet; digitale Signaturen und Infrastrukturen zum Management öffentlicher Schlüssel (PKI) erlauben die Feststellung und das Verbergen der Identität. Technologien für Transparenz und Kontrolle sind in Ansätzen sichtbar. Die Herausforderung dabei ist, dass zum einen nur der Zugang zu den eigenen Daten gewährleistet werden soll und zum anderen durch die Ableitung von möglichen Gesetzmäßigkeiten der Bereich zu identifizieren ist, in dem persönliche Daten Wirkung erzielt haben.

Während zur Ermittlung der Beziehungen von Schutzzielen und deren Verletzung durch die Datenverwendung bereits Methoden von einfachem „Pattern Matching" bis hin zu „Complex Event Processing" existieren, ist die personalisierte Evidenzgenerierung, insbesondere die Garantie der Vollständigkeit und Abwesenheit von „false negatives", eine bislang ungeklärte Forschungsfrage.[372]

3.2.3 SCHUTZ

Bezüglich der Herstellung von Transparenz und Kontrolle existieren technische, rechtliche, aber auch wirtschaftspolitische Probleme. Transparenz bedingt die Einsicht in die Abläufe und verlangt damit die Preisgabe der Grundlagen eines Geschäftsmodells. Statistische Genauigkeit, wie sie in Wirtschaftsinformatik und Betriebswirtschaftslehre praktiziert wird, reicht zwar für wirtschaftliche Belange aus, kann jedoch Privatheit im Sinne einer rechtlichen oder ethischen oder auch nur aktuell technischen Betrachtungsweise nicht garantieren. Im technischen Bereich geht es um die Überprüfung der Einhaltung von Schutzzielen. Sicherheitsmonitore können während der Ausführung Schutzziele überprüfen.[373] Die Grenze liegt in der zyklischen Verbundenheit der Transaktionen. Hierfür müssten die Monitore bei jeder Transaktion einschätzen, ob diese über gemeinsame Daten mit anderen Transaktionen verbunden ist. Wenn der vollständige Ablauf von Überwachung nicht garantiert werden kann, bleibt die Nutzungskontrolle unwirksam.

Für Privatheitsanforderungen, die nicht durch Monitore, also schon vor oder während der Ausführung durchgesetzt werden sollen, verbleiben entweder statische Ablaufanalysen oder forensische Verfahren. Diese analysieren die Aufzeichnungen der Aktivitäten und stellen fest, ob zum Beispiel gegen Vorgaben des BDSG verstoßen wurde. Privatheitsverletzungen können zwar nicht verhindert, aber nachträglich erkannt werden. Die Kontrolle der Kontrolleure bleibt ungeklärt.

Privacy Enhancing Technologies (PET) ist der Sammelbegriff für alle privatheitsgarantierenden Mechanismen. Sie basieren alle auf der Einhaltung von Sicherheitseigenschaften, die zum einen bekannt sind und zum anderen bei Verletzung nicht zum Zugang zu Daten führen. Eine Ausnahme sind die forensischen Techniken. Es ist eine unbestreitbare Erkenntnis, dass die PET-Verfahren nur eine geringe Akzeptanz bei den Nutzern gefunden und damit die Privatheit nicht erhöht, sondern ihr in Einzelfällen eher geschadet haben,[374] da man an der Wirksamkeit der Technik und an deren Nutzerfreundlichkeit zweifelt. Während

372 Accorsi 2008a.
373 Pretschner / Hilty / Schaefer et al. 2008.
374 Benisch / Kelley / Sadeh / Cranor 2011.

PET auf die Einhaltung von Datensparsamkeit bestehen, ist das Geschäftsmodell der Web 2.0-Dienste auf das Sammeln und Auswerten von Daten angelegt. Die Ziele von PET und Web 2.0 widersprechen sich. PET Mechanismen benötigen konkrete Spezifikationen, um eine Verletzung von Obligationen zu verhindern, während Geschäftsmodelle immer auf der Suche nach neuen Chancen sind. Das Web 2.0 soll für Kunden Gutes ermöglichen, während Privatheitsmechanismen Schlechtes verhindern. Die Ursache für die Nutzung von datenzentrischen Diensten sind Anreize und nicht Besorgnisse. PET sind Technologien zur Abwehr von Gefahren.

Privatheit unterscheidet sich zudem von Sicherheit. Letztere befasst sich mit der Verschlüsselung von Daten, sodass diese allen denen verborgen bleiben, die keinen Zugang erhalten sollen. Voraussetzung dafür ist, dass Kommunizierende sich vertrauen, während Interakteure sich bei der Forderung nach Privatheit eben nicht vertrauen. Man möchte ja gerade, dass ein anderer etwas nicht erfährt. Die Datensparsamkeit als Grundlage der rechtlichen Regelungen plädiert dafür, dass man nichts an Daten freigibt, wenn es die Sache nicht erfordert. Die PET versetzen den Nutzer theoretisch in die Lage, das Interaktionsverhältnis zu kontrollieren. Allerdings gilt dies nur solange, wie der Anbieter die Dienstbereitschaft aufrechterhält. Bezüglich der PET sind drei Konzepte zu unterscheiden:

1. Die Identitätskontrolle stellt Verfahren zur Authentifikation bereit, die bei positivem Ausgang einen Zugang zu den Daten oder Diensten ermöglichen und gleichzeitig über Pseudonyme und Anonymität ein hohes Maß an Datensparsamkeit zulassen. Dennoch gibt es am Ende der Kette den Punkt, an dem Pseudonymität und Anonymität aufgelöst werden müssen, um einen Tausch von Gütern zu ermöglichen. All diese Verfahren basieren auf der sogenannten PKI (Public Key Infrastruktur), die in Deutschland die Grundlage des digitalen Personalausweises und aller weiteren Karten ist. Sie ist gesetzlich im Signaturgesetz geregelt.

2. Die Nutzungskontrolle ergänzt die Verfahren zur Regelung der Zugangskontrolle durch die Überwachung der Handlungen nach dem Datenzugriff. In einer Freiburger Umfrage zeigt sich, dass über 80 Prozent der Nutzer private Daten abgeben würden, wenn sie sich sicher wären, dass sie in die vereinbarte Verwendung ihrer Daten vertrauen könnten.[375] Sichere Mehrparteienkommunikation ist das Ziel des Sicherheitsmodells nach Yao.[376] Es geht um die minimale Preisgabe von Daten zum Schutz der Verhandlungsposition. Im engen Sinne ist dies keine Frage nach Privacy, da man persönliche Daten nicht dauerhaft schützen möchte, sondern man um die Aufgabe von informationellen Vorteilen zum Beispiel bezüglich der Verhandlungsposition fürchtet. Die ordnungspolitische Problematik liegt in der potenziellen Kontrolle von persönlichen und juristischen Personen.

3. Die forensische Kontrolle verzichtet vollständig auf den Schutz von persönlichen Daten, zeichnet im Gegenzug aber alle Nutzungen der Daten samt deren Verursacher auf. Sollten Vereinbarungen zwischen Anbieter und Nachfrager getroffen sein (security policies), können Verletzungen zwar nicht verhindert, aber entdeckt und potenziell sanktioniert werden. Der Nachteil ist, dass die Aufzeichnung ein lohnenswertes Objekt für Privatheitsverletzungen darstellt.[377]

Zur Anonymität hat Chaum Möglichkeiten und Grenzen technisch definiert.[378] Anonymität behindert Interaktion und damit wirtschaftliche Tätigkeit. Sie ist als Technik für eine neue Vertrauensinfrastruktur wirtschaftlich eher unwesentlich, wie aus Abbildung 1 zu ersehen ist.

375 Kaiser / Reichenbach 2002.
376 Yao 1982.
377 Accorsi 2008a.
378 Chaum 1981.

Der Einsatz von PET ist eine Funktion des Aufwands, der für Privatheit für sinnvoll erachtet wird. Anonymität ist demnach oft ökonomisch von Nachteil, da die Kosten für die Informationsbeschaffung und für die Koordination von Angebot und Nachfrage steigen. Der Wert der PET ist demzufolge nur im Schaden zu messen, den eine Nichtanwendung bedeutet. Der Schutz der Privatheit ist in Abhängigkeit vom möglichen persönlichen Ertrag zu sehen. Garantiert die IT-Infrastruktur die Einhaltung von Schutzzielen, ist sie im informatischen Sinne technisch sicher.[379] Zwei Eigenschaften moderner IT-Infrastrukturen machen es nahezu unmöglich, vorgeplante Privatheit einzuhalten, wie sie in PET notwendige Bedingung sind:

1. Die Umsetzung einer vertrauenswürdigen Zugriffskontrolle würde mit den gegenwärtigen Mechanismen einen zentralen und globalen Vertrauensanker voraussetzen,[380] der selbst wieder nicht zu 100 Prozent sicher wäre.

2. Das Internet ist hochdynamisch und ermöglicht so die spontane Vernetzung von Personen und Prozessen, um wechselnde wirtschaftliche Ziele zu erreichen. PET basiert auf vorigen Absprachen und schließt Spontanität aus. So begrenzen PETs die wirtschaftliche Dimension von datenzentrischen Diensten auf die Gutwilligkeit von Akteuren, ihre Absichten bekanntzugeben und doch zu wissen, dass sie bei diesem Versprechen ohne Systemüberblick handeln.[381]

3.2.4 NUTZEN

Ausgangspunkt zur Diskussion des Nutzerverhaltens von datenzentrischen Diensten ist die sich empirisch erhärtende Beobachtung, dass die Anwender durchaus über das zweiwertige, verzögerte Erlösmodell nach Abbildung 2 Kenntnis haben, sich aber trotzdem in überwiegender Zahl für die Nutzung der Dienste entscheiden. Das Nutzerverhalten, das durch die Delegation von potenziellen wirtschaftlichen Nachteilen in der Zukunft aufgrund des Nutzens im Jetzt charakterisiert werden kann, wird auch vielfach als „Paradox" bezeichnet, das man bekämpfen müsse. Schlagworte dazu sind der den mündigen Nutzer ermöglichende „Internetführerschein" oder eben eine Technik, die automatisiert den Schutz übernimmt, da man den Nutzer für dazu nicht fähig hält oder glaubt, dass dieser einen solchen Schutz nicht wolle und man ihn zum Glück zwingen müsse. Trotz aller Bemühungen in den letzten zehn Jahren zeigen nahezu alle Untersuchungen, dass von 1998 bis heute die Verhaltensweisen der Nutzer in etwa gleich geblieben sind. Danach sind etwa 25 Prozent der Nutzer trotz aller Schulungen eher unwillig, in die Nutzung von PET zu investieren. Die Motivation ist dabei zu je gleichen Teilen eine Abstinenz von den Diensten oder eine optimistische Einschätzung der Gefahren der Datenverwendung. 50 Prozent der Nutzer sind als an der Privatheit interessiert zu bezeichnen. Sie sind aber ebenso wie die Optimisten nicht bereit, über ein Minimum ihrer Zeit und über ein Minimum intellektueller Vorbereitung hinaus in die Nutzung des Internets zu investieren. Die verbleibenden 25 Prozent aller Nutzer ziehen es vor, wegen der Privatheitsbedenken nur solche Dienste zu nutzen, die keine persönlichen Daten verlangen.[382]

Datenzentrische Dienste geben den Anwendern und ihren Kunden einen konkreten Nutzen. Ihr Geschäftsmodell kann in vier Komponenten zerlegt werden:

1. Rahmenbedingungen: In Deutschland werden zurzeit in zunehmendem Umfang ca. 20 Prozent des Wirtschaftswachstums mittel- und unmittelbar mit dem Internet erzeugt. Die Informationsverarbeitung und das Zusammenführen von Optionen werden zum dominanten Aspekt der Wertschöpfung. Datenzentrische Dienste senken die Suchkosten für alle.

379 Müller / Rannenberg 1999.
380 Accorsi / Sato / Kai 2008.
381 Müller 2008.
382 Kaiser 2003.

2. Angebot und Innovation: Datenzentrische Dienste innovieren entweder über das Angebot, den Preis oder über den Prozess. Gegenwärtig ist der Wettbewerb zwischen Web 2.0-Diensten tendenziell angebotsorientiert und findet über Innovationen statt. Allerdings bestehen auf Teilmärkten bereits jetzt Quasi-Monopole.

3. Kundenbeziehung: Wissen über Kunden erlaubt eine optimale Bedienung der Kundenwünsche und damit die Reduktion von Fehleinschätzungen. Datenzentrische Dienste sind aktuell die günstigste Form, um CRM zu ermöglichen.

4. Erlöse: Das Erlösmodell datenzentrischer Dienste erlaubt Dritten den Zugang zu Datenaggregationen mit den prominenten Einsatzbedingungen Werbung, Preisdifferenzierung und Inferenzen. Die Daten werden dabei nicht notwendigerweise an Dritte verkauft, gegenwärtig führend ist die Nutzung über eine Plattform.

Datenzentrische Dienste, die nach Wirksamkeitskriterien wie Kosten per Klick (Cost-per-Click oder CPC) bemessen werden, haben dabei einen Kostenvorteil im Vergleich zu den Erlösmodellen klassischer Werbung, die nach Reichweite kalkulieren. Der Kontaktpreis für 1000 Personen (TKP), der für herkömmliche Werbung anfällt, ist wesentlich unschärfer als die klickbasierten Abrechnungsmodelle datenzentrischer Dienste. Kosten, die nach Klick, Lead oder Auftrag kalkuliert werden, erlauben analog zur personalisierten Ansprache der Kunden eine leistungsbezogene Abrechnung der Effektivität personalisierter Werbung. Der Kunde bekommt davon oft nichts mit. Bislang hat dieses Interaktionsverhalten zur Steigerung der wirtschaftlichen Produktivität geführt.[383]

3.3 PRIVATHEIT: SZENARIO E-COMMERCE

Vertrauensinfrastrukturen und Privatheit sind abhängig vom wirtschaftlich relevantesten Szenario, das idealerweise durch die Produktivitätssteigerungen die Kosten der zusätzlichen Privatheitsinvestitionen tragen können. Bislang ist trotz des aktuellen Hypes um das Web 2.0 der E-Commerce zu über 80 Prozent für die Produktivitätsbeiträge verantwortlich. In einer der umfassendsten Studien zur Bedeutung des Internets als wirtschaftlich relevante Infrastruktur – durchgeführt an der Universität Freiburg – wurde im Jahre 2005 gezeigt, dass klassische Unternehmen der „Old Economy" durch das Internet modernisiert wurden. Da der Mythos der „New Economy" den Internethype bis zum Jahre 2000 befeuert hat, ist man heute zu objektiven Aussagen zur Wirkung des E-Commerce fähig und konstatiert, dass es sich letztlich um eine gigantische Produktivitätsverbesserung der „Old Economy" gehandelt hat. Die Produktivitätspotenziale des E-Commerce liegen damit in ihrer Mehrheit aufseiten der Anbieter und weniger bei den Kunden.

3.3.1 SAMMLUNG VON DATEN

In der ECE-Studie aus dem Jahr 2005 wurde neben Nutzungsfeldern auch nach der Erhebung und Verwertung kundenspezifischer Daten gefragt. Entscheidungsträger der oberen Managementebenen deutscher Unternehmen (vorwiegend mittlere und Großunternehmen, aber auch Kleinunternehmen, klassifiziert nach Branchen)[384] äußerten zwar großes Interesse an der Erhebung und Nutzung persönlicher Daten, nicht zuletzt als zukünftige Grundlage zur weiteren Individualisierung von Produkten oder Dienstleistungen. Allerdings wurden die Fähigkeiten hierfür als gering und der Umfang im Verhältnis zu den Kosten als unzureichend eingeschätzt. So werteten 65,2 Prozent aller

383 Brynjolfsson / Saunders 2010.

384 Branchenverteilung: B2B Dienstleistungen (25,1 %), Verarbeitendes Gewerbe (22,7 %), Handel (16,3 %), Baugewerbe (9,1 %), Sonstige Dienstleistungen (7,9 %), Verkehr- und Nachrichtenübermittlung (6,8 %), Gastgewerbe (4,1 %), Kredit- und Versicherungsgewerbe (3,7 %), Landwirtschaft (2,6 %), Energie- und Wasserversorgung (1,7 %).

Tabelle 3: Nutzung und Sammlung kundenspezifischer Daten[385]

	DATEN WERDEN GENUTZT	DATENNUTZUNG GEPLANT	DATEN WERDEN NUR GESAMMELT
Zahlungsverhalten	51,7 %	4,7 %	13,0 %
Kaufhistorie	45,6 %	7,0 %	13,9 %
Soziodemografische Daten	17,6 %	6,3 %	14,4 %
Surfverhalten	6,3 %	3,4 %	10,4 %
Andere Daten	29,0 %	3,3 %	9,9%

Unternehmen vornehmlich Zahlungsverhalten und Kaufhistorie ihrer Kunden aus und nutzten diese Informationen beim wiederholten Kundenkontakt (siehe Tabelle 3).

Knapp über ein Drittel der Unternehmen (34,5 Prozent) setzte hierfür unternehmensweite CRM- (Customer Relationship) oder ERP-Systeme ein, mittels derer die kundenspezifischen Daten aus unterschiedlichen Unternehmensbereichen zusammengeführt und ausgewertet werden. Weitere 8,7 Prozent waren zum Zeitpunkt der Veröffentlichung der Studie gerade dabei, ein solches System aufzubauen oder planten, dies in den darauffolgenden zwei Jahren zu tun.

Das am häufigsten genutzte Merkmal ist das bisherige Zahlungsverhalten der Kunden, das von 51,7 Prozent der Unternehmen bereits genutzt und von weiteren 4,7 Prozent zu erheben geplant wurde. Die branchenspezifische Auswertung ergab ein interessantes Bild. Hier fielen vor allem die Branchen Gastgewerbe und Handel als Daten-Nachfrager auf. Bei der Nutzung von Informationen über das Zahlungsverhalten ihrer Kunden lag der Handel mit 61,2 Prozent (Basis 85) deutlich über dem Durchschnitt. Im Gastgewerbe sammelten mit einem Anteil von 45,5 Prozent (Basis 22) verglichen mit dem Gesamtdurchschnitt mehr als dreimal so viele Unternehmen Daten über das Zahlungsverhalten ihrer Kunden, ohne diese konkret zu nutzen. In der Branche Verkehr und Nachrichtenübermittlung waren die diesbezüglichen Planungen bei 15,2 Prozent (Basis 33) der Unternehmen mit Abstand am größten.

Fast gleichauf wurde die Kaufhistorie der Kunden von 45,6 Prozent der Unternehmen ausgewertet. Der Anteil der Unternehmen, die eine diesbezügliche Nutzung planten, lag bei 7,0 Prozent. Auch hier hob sich die Handelsbranche (60,0 Prozent, Basis 85) zusammen mit dem Gastgewerbe (63,6 Prozent, Basis 22) deutlich vom Durchschnitt ab. Das Gastgewerbe war auch bei der Sammlung von Kaufhistorien ohne konkrete Nutzung Spitzenreiter; dort lag der Anteil bei 22,7 Prozent und damit deutlich über dem Durchschnitt von 13,9 Prozent. Für die nahe Zukunft planten vor allem Unternehmen aus dem Kredit- und Versicherungsgewerbe, die Kaufhistorie ihrer Kunden zu nutzen, der Anteil lag hier mit 21,1 Prozent (Basis 19) weit über dem Durchschnitt von 7,0 Prozent.

Die Verwendung soziodemographischer Daten fiel dagegen relativ gering aus. Insgesamt nutzten 17,6 Prozent der Unternehmen soziographische Daten wie Alter, Geschlecht oder Bildungsstand ihrer Kunden. Herausragend ist hier vor allem das Kredit- und Versicherungsgewerbe, da in dieser Branche 52,6 Prozent der Antwortenden angaben, soziografische Daten zu verwenden. Schon etwas abgeschlagen, aber immer noch weit über dem Durchschnitt, waren die

[385] Sackmann / Strüker 2005.

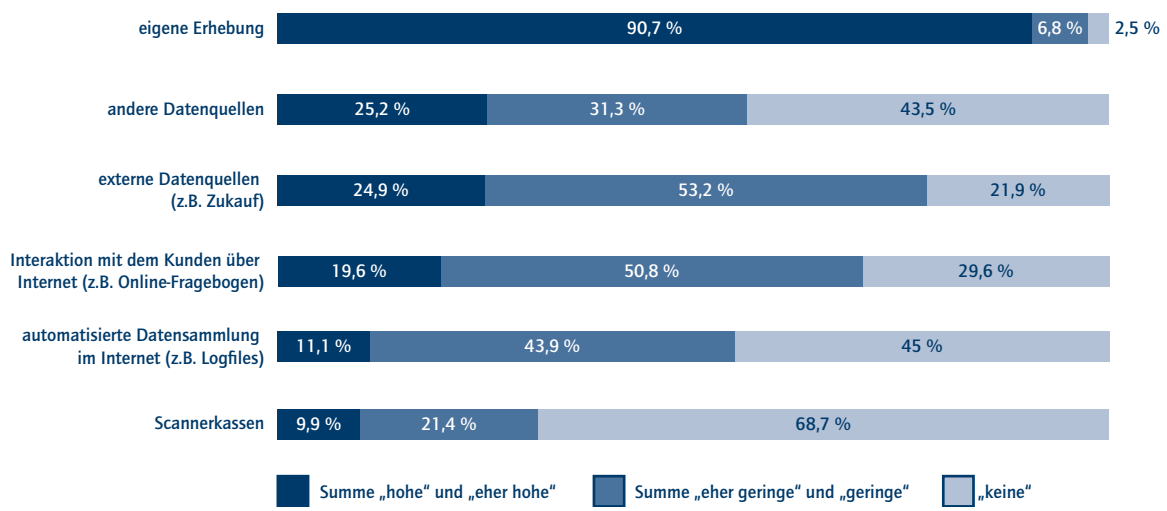
Branchen Sonstige Dienstleistungen mit 30,8 Prozent und der Handel mit 25,9 Prozent zu finden. Das Gastgewerbe stand auch bei der Sammlung soziodemographischer Daten mit einem Anteil von 42,9 Prozent (Basis 21) an der Spitze.

Die Auswertung des Surfverhaltens im Internet wurde lediglich von 6,3 Prozent der Unternehmen vorgenommen und genutzt. Hier ließen sich zwischen den einzelnen Branchen kaum Unterschiede feststellen. Jedoch ist auch hier das Gastgewerbe sowohl bei der Nutzung als auch bei der Sammlung von Daten führend.

Als Informationsquelle für kundenspezifische Daten spielen in deutschen Unternehmen Eigenerhebungen eine zentrale Rolle. 90,7 Prozent der Unternehmen sahen deren Bedeutung als hoch oder eher hoch an. Der Zukauf externer Daten hatte – schon weit abgeschlagen – für insgesamt 24,9 Prozent der Unternehmen eine hohe oder eher hohe Bedeutung. Im Kredit- und Versicherungsgewerbe lag dieser Anteil mit 42,9 Prozent besonders hoch. Für den Handel hingegen fiel der entsprechende Anteil mit 17,6 Prozent beziehungsweise 21,1 Prozent für die Teilbranche Einzelhandel überraschend gering aus. Lediglich beim Zukauf externer Daten ließ sich ein Zusammenhang zwischen der Einschätzung der Unternehmen und der Unternehmensgröße feststellen. So ist der Anteil bei Großunternehmen mit 37,0 Prozent mehr als doppelt so hoch wie in der Gruppe der Klein- und Kleinstunternehmen (16,9 Prozent).

Eine Interaktion mit den Kunden über das Internet, zum Beispiel anhand eines Online-Fragebogens, stellte für 19,6 Prozent der Unternehmen eine Informationsquelle mit hoher oder eher hoher Bedeutung dar. Hier hoben sich vor allem das Gastgewerbe und die B2B-Dienstleister von den restlichen Branchen positiv ab. Die automatisierte Datensammlung im Internet beispielsweise über die Analyse von Logfiles spielte für ca. jedes neunte Unternehmen (11,1 Prozent), das kundenspezifische Daten auch nutzte, eine bedeutende oder eher bedeutende Rolle. Unternehmen aus den Branchen Handel, Gastgewerbe und Dienstleistungen führten hier das Feld an. Auch ließ sich ein klarer positiver Zusammenhang zur Dauer der eigenen Internetpräsenz feststellen. Scannerkassen

Abbildung 4: Informationsquellen kundenspezifischer Daten[386]



386 Sackmann / Strüker 2005.

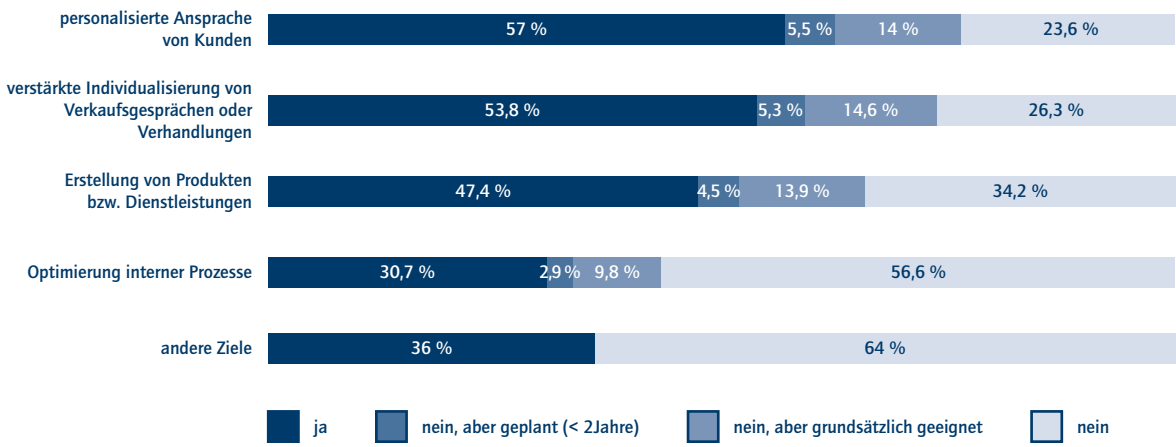
spielten für 9,9 Prozent der Unternehmen eine bedeutende oder eher bedeutende Rolle bei der Erhebung kundenindividueller Daten. Wie zu erwarten fanden sich in dieser Gruppe vor allem Unternehmen aus dem Handel wieder. Der Anteil der Unternehmen, die Scannerkassen hierbei eine hohe oder eher hohe Bedeutung zugemessen haben, lag im Handel bei 37,0 Prozent (Basis 73), in der Teilbranche Einzelhandel bei 57,8 Prozent (Basis 38).

3.3.2 VERWENDUNG VON DATEN

Die Ziele, die die Unternehmen mit der Erhebung kundenspezifischer Daten verfolgten, sind primär die Verbesserung des Kundenkontakts (siehe Abb. 5). 57,0 Prozent der Unternehmen setzten die verfügbaren kundenspezifischen Daten zur personalisierten Ansprache ihrer Kunden ein, beispielsweise zur Erstellung von Angeboten mit individuellen Preisen, zur Gewährung besserer Konditionen für gute Kunden oder bei der Nachbetreuung von Kunden. Weitere 5,5 Prozent wollten eine solche Nutzung innerhalb der kommenden zwei Jahre realisieren. Der Anteil der Unternehmen, die die kundenspezifischen Daten zur verstärkten Individualisierung von Verkaufsgesprächen oder Verhandlungen nutzten, lag bei 53,8 Prozent, weitere 5,3 Prozent planten eine solche Nutzung. Der Erfolg dieser Aktivitäten lässt sich daran erkennen, dass in beiden Fällen über die Hälfte der bereits aktiven Unternehmen plante, seine diesbezüglichen Aktivitäten auszuweiten und nur ca. jedes Zwanzigste diese wieder einschränken wollte.

Bei der Individualisierung der Kundenkontakte in der Ansprache oder für die Gestaltung von Verkaufsgesprächen hatte die Kommunikation individualisierter Zusatzinformationen, wie beispielsweise Einkaufstipps, für 59,5 Prozent der Unternehmen eine hohe oder eher hohe Bedeutung. Gleichauf wurde der Unterbreitung exklusiver Angebote von 59,3 Prozent der Unternehmen eine hohe oder eher hohe Bedeutung zugemessen. Etwas geringer fielen die entsprechenden Anteile bezüglich der Einschätzung der Möglichkeiten einer personalisierten Preisgestaltung beispielsweise in Form individueller Rabatte (50,4 Prozent) und der Vereinbarung persönlicher Zusatzleistungen beispielsweise in Form einer Garantieverlängerung (51 Prozent) aus.

Abbildung 5: Ziele der Nutzung kundenspezifischer Daten[387]



[387] Sackmann / Strüker 2005.

Einen Einfluss auf die Erstellung von Produkten beziehungsweise Dienstleistungen, wie beispielsweise zur individuellen Ausgestaltung, hatten kundenspezifische Daten bei 47,4 Prozent der befragten Unternehmen. Auch hier liegt der Anteil der Unternehmen, die ihre bisherigen diesbezüglichen Aktivitäten ausweiten wollten, bei über der Hälfte. Die Nutzung kundenspezifischer Daten zur Optimierung interner Prozesse wurde immerhin noch von 30,7 Prozent der befragten Unternehmen angestrebt, weitere 2,8 Prozent planten eine solche Aktivität für die nahe Zukunft.

Aus einzelwirtschaftlicher Sicht können für E-Commerce zwei Entwicklungsschritte unterschieden werden, die bei identischem wirtschaftlichem Szenario und Geschäftsmodell völlig unterschiedliche Auswirkungen auf die Gewährung von Privatheit haben. Ausgehend von der unternehmenszentrischen Sicht entwickeln sich durch die verteilte Wertschöpfung zunehmend kooperative Formen des E-Commerce, die als Vorgänger zu den datenzentrischen Diensten des Web 2.0 gesehen werden können:

A: Unternehmenszentrische Sichtweise

Die Wirksamkeit von Sicherheits- und Privatheitsmechanismen wird durch ihren Gültigkeitsbereich oder Perimeter bestimmt. Sind diese mit den Grenzen einer Organisation identisch, spricht man von der unternehmenszentrischen Sichtweise. Die Hürden, die die befragten Unternehmen bezüglich einer Erhebung oder Nutzung kundenspezifischer Daten sahen, lagen vor allem in der Integration solcher Maßnahmen in bestehende Abläufe und in die bestehende IT-Infrastruktur. Jeweils 43,6 Prozent sahen darin eine hohe oder eher hohe Hürde. Der Anteil der Unternehmen, die ein negatives Kosten-Nutzen-Verhältnis erwarteten, lag bei 42,0 Prozent. Über ein Drittel (37,3 Prozent) befürchteten zudem negative Kundenreaktionen aufgrund einer potenziellen Verletzung ihrer Privatsphäre, allerdings benannten lediglich 20,9 Prozent einen möglichen Image- oder Reputationsverlust als hohe oder eher hohe Hürde. Auch wurde von 34,2 Prozent eine geringe Akzeptanz der Datenerhebung und Datennutzung aufseiten der Kunden befürchtet. Datenschutzrechtliche Bedenken wurden von 34,4 Prozent, sonstige rechtliche Bedenken von 22,6 Prozent als hohe oder eher hohe diesbezügliche Hürde angesehen.[388]

Die Hürden in Bezug auf die Dauer der Internetpräsenz wurden vor allem von den Unternehmen, die erst seit den letzten drei Jahren vor der Befragung im Internet präsent waren, als überdurchschnittlich hoch eingeschätzt. Während bei den Unternehmen, die länger als sieben Jahre über eine Internetpräsenz verfügten, der Anteil bei 38,7 Prozent lag, sehen 47,1 Prozent der Einsteiger diesbezüglich hohe oder eher hohe Probleme. Dieses Verhältnis verschob sich bei der Einschätzung der rechtlichen Hürden; so sehen bezüglich des Datenschutzes die Unternehmen, die länger als sieben Jahre im Internet präsent waren, mit einem Anteil von 38,0 Prozent hohe oder eher hohe Hürden, bei den erst seit kurzem präsenten Unternehmen lag der Anteil bei 32,6 Prozent.

Bemerkenswerte Ergebnisse lieferte auch eine differenzierte Betrachtung der Einschätzung zwischen denjenigen Unternehmen, die bereits kundenspezifische Informationen nutzen, und denjenigen, die dies bisher noch nicht taten. Der größte Unterschied zeigte sich bezüglich der Einschätzung eines möglichen Image- oder Reputationsverlustes. Dieses Szenario wird von 27,1 Prozent der Unternehmen, die keine kundenspezifischen Daten sammeln oder nutzen, als hohe oder eher hohe Hürde angesehen; bei den bereits aktiven Unternehmen lag der entsprechende Anteil bei lediglich 17,4 Prozent. Dies könnte als Hinweis gewertet werden, dass Unternehmen, die kundenspezifische Daten nutzen, hierdurch auch für den Kunden einen realen Mehrwert geschaffen haben und daher das Szenario eines Imageverlustes aufgrund der bisher gemachten Erfahrungen als nicht so bedrohlich ansahen. Jedoch konnte bezüglich der Hürde „Zu erwartende negative Kundenreaktionen aufgrund der Verletzung ihrer Privatsphäre" kein entsprechender Unterschied festgestellt werden (siehe Tabelle 4).

[388] Sackmann / Strüker 2005.

Tabelle 4: Hürden nach Nutzung kundenspezifischer Daten [389]

HÜRDE	UNTERNEHMEN, DIE KUNDENDATEN SAMMELN UND NUTZEN BASIS 280-267	UNTERNEHMEN DIE *KEINE* KUNDENDATEN SAMMELN ODER NUTZEN BASIS 147-140
Aufwendige Integration in bestehende IT-Infrastruktur	40,1 %	48,6 %
Aufwendige Integration in bestehende Abläufe/Organisation	41,4 %	46,3 %
Möglicher Image- oder Reputationsverlust	17,4 %	27,1 %
Erwartete negative Kundenreaktion aufgrund einer Verletzung ihrer Privatsphäre	37,0 %	37,7 %
Datenschutzrechtliche Bedenken	32,0 %	37,7 %
Kosten übersteigen den Nutzen	38,6 %	46,4 %

Etwas überraschend war, dass die Einschätzung dieser beiden Hindernisse so unterschiedlich ausfällt. Auszeichnungen wie der „Big Brother Award" und ihre Wirkungen auf das Unternehmensimage legen die Vermutung nahe, dass eine Verletzung der Privatsphäre der Kunden auch eine Bedrohung für das Unternehmensimage darstellt. Der Anteil der Unternehmen, die wegen der Nutzung personenbezogener Daten einen Imageverlust befürchteten (hohe oder eher hohe Hürde), ist jedoch wesentlich geringer, als bei der Hürde „Erwartete negative Kundenreaktion aufgrund Verletzung ihrer Privatsphäre".

B: Kooperative oder de-perimetrisierte Sichtweise

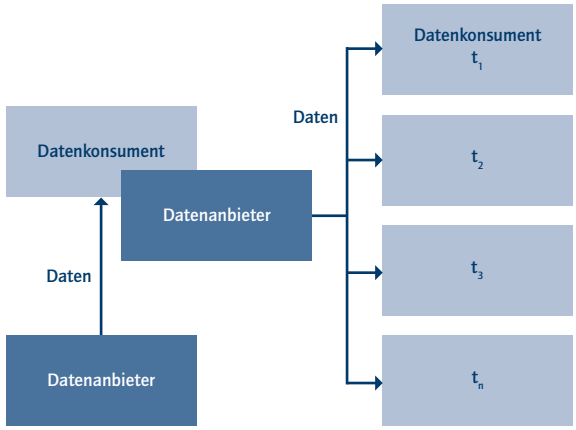
Sobald der Perimeter eines Unternehmens überschritten wird und für eine gemeinsame Zielerreichung wechselnde, de-perimetrisierte Teilnehmer kooperieren, spricht man von einer kooperativen Sichtweise auf Privatheit und Sicherheit von Daten. E-Commerce ist für Unternehmen primär und in seiner einfachsten Form ein günstiger und zusätzlicher Vertriebskanal. Man profitiert von der besseren Kenntnis von Kunden in weit geringerem Maße als von der Rationalisierung des Kaufprozesses durch die Entbindung von Raum und Zeit. Die Nutzung dieses Potenzials führte in der weiteren Entwicklung des E-Commerce zu seiner kooperativen Form, wobei die Einzelphasen der Transaktion nicht mehr unbedingt durch dieselbe Unternehmung vertreten werden müssen. Die Verteilung der Wertschöpfung erfordert eine erhöhte Koordination, was in der Internetökonomie durch Wissen um Zusammenhänge in bisher unbekanntem Umfang erreicht wird. Im klassischen E-Commerce stammten Daten noch vorwiegend aus Eigenerhebungen (vgl. Abb. 4). Kooperative Werterstellung haben die Anforderungen zur Spezialisierung von Diensten gegeben, die sich ausschließlich über Datenaggregation koordinieren lassen. Wie aus Tabelle 4 zu entnehmen, lagen 2005 die größten Hürden zur Realisierung des E-Commerce in der Sammlung und Verwertung von Kundendaten bei einer aufwendigen Integration sowohl in bestehende IT-Infrastrukturen als auch in bestehende Geschäftsprozesse. Dies galt für Unternehmen, die bereits kundenspezifische Daten nutzten und solche, die dies zum damaligen Zeitpunkt (noch) nicht taten. Bei letzterer Gruppe dominierten die hohen Kosten im Verhältnis zum Nutzen kundenspezifischer Daten. Aktuelle Studien belegen den Abbau der Hürden, die noch 2005 der Sammlung und Verwertung von Kundendaten im Wege standen. Barrieren, wie die aufwendige

[389] Sackmann / Strüker 2005.

Integration der Datensammel- und Verwertungspraxis in die IT-Infrastruktur sowie in bestehende Abläufe und Organisationsstrukturen, wurden in den letzten Jahren durch neue IT-Trends wie Cloud Computing[390] und den Aufbau von Organisational Capital,[391] zum Beispiel Reorganisation der Geschäftsprozesse, innerbetrieblich abgebaut.

Die Standardisierung und Professionalisierung der Datensammlung macht diese zu einem Unterstützungsdienst für Unternehmen des E-Commerce und auch der „alten" Ökonomie. Datenaggregationen reduzieren Medienbrüche und senken Kosten dann, wenn die Daten gleichzeitig zielgenauer sind, wozu neuartige Formen der Erhebung vorhanden sein müssen. Besonders Technologien, die dem Web 2.0 zuzurechnen sind (Blogs, Wikis, Social Networks), sind dafür ideal geeignet. Sie reduzieren die Erhebungskosten durch eine generelle Verwendbarkeit der Daten, vorausgesetzt, eine hilfreiche Analytik ist verfügbar. Während 2005 lediglich 6,3 Prozent der deutschen Unternehmen Daten zum Surfverhalten ihrer Kunden genutzt haben, hat sich die Erhebung und Auswertung von Klickdaten, begünstigt durch die kooperativen Dienste vervielfacht.[392] Vor gut einem halben Jahrzehnt spielte die automatisierte Datensammlung und Auswertung von Logfiles nur für jedes neunte Unternehmen (11,1 Prozent), das kundenspezifische Daten auch nutzte, eine bedeutende oder eher bedeutende Rolle. Heute hingegen werten Unternehmen jeglicher Branche und Größe mittels Analyse-Tools die Besucherzahlen und Klickdaten ihrer Online-Auftritte aus.

Abbildung 6: Rollenverständnis bei Unterstützungsdiensten



Zunehmend werden heute Daten in wirtschaftlicher Absicht und mit Wertvorstellungen in der Angebotsproduktion eingesetzt.[393] Damit verschiebt sich das Problem des Schutzes von Privatheit – weg vom Besitzer einer Informationsressource, wie zum Beispiel beim Client-basierten E-Commerce, hin zum Schutz des Kunden. Der Kunde wird zum Datenanbieter, der datenzentrische Dienst zur ersten Stufe einer Reihe von Datenkonsumenten (siehe hierzu Abb. 6).

Der Konsument datenzentrischer Dienste wird in Wahrheit zum Datenanbieter von Konsumentendaten, während die Datensammler zu den wahren Datenkonsumenten werden. Dies hat Folgen für die Privatheitsmechanismen. Es sind nicht mehr die PET, die Privatheit ermöglichen. Stattdessen sollte die Fortentwicklung der PET zu TET[394] (Transparency Enhancing Technology) „Transparenz" und „Kontrolle" oder aus wirtschaftlicher Sicht, „Signalling" und „Screening" bereitstellen, um dem Kunden eine Entscheidung über den Wert von Privatheit zu ermöglichen.

3.4 PRIVATHEIT: SZENARIO KOOPERATIVE DIENSTE

Kooperative Dienste sind verbesserte Formen der Interaktion mit den Teilnehmern am E-Commerce, indem Dienste angeboten werden, die sich nicht nur auf die Bereitstellung eines

390 Armbrust 2009.
391 Brynjolfsson / Saunders 2010.
392 IWF 2011.
393 Anderson 2010.
394 Böhme 2008.

Vertriebskanals stützen. Gegenwärtig dominante Nutzungsformen des Internets sind Plattformen für den Datenanbieter, die für ihn attraktive Dienste für den Arbeits-, Freizeit- und den sozialen Bereich bereithalten und in der Tat zu einem Nervensystem der gesellschaftlichen Kommunikationsformen geworden sind. Die Einbindung der Nutzer und die Fusion aller Lebensbereiche in einem Medium erlaubt eine nahezu vollständige Einsicht in die Lebenswelt des Kunden. Aufgrund dieser Kenntnisse können Fehlplanungen vermieden und zusätzlich neue Optionen entdeckt werden sowie die alten Funktionen des E-Commerce noch günstiger abgedeckt werden. Prinzipiell wird die Idee verfolgt, die Bonität des Kunden besser einschätzen zu können und dabei die freien Valenzen zu entdecken. Diese frei verfügbaren Mittel und die Neigung der Kunden sind das Maß für die Effizienz und Neuartigkeit der Web 2.0-Dienste aus wirtschaftlicher Sicht. Dabei unterscheiden sich die Angebote dieser Dienste hinsichtlich E-Commerce in sieben wichtigen Punkten:

1. Dienste werden nicht mehr als verpackte Software mit Lizenznummer vertrieben, die man mit traditionellem Kaufverhalten erwirbt, sondern Dienste stehen kostenlos online zur Verfügung.

2. Die Kontrolle über korrekte und schwer zu erhaltende Datenquellen ist die Triebfeder hinter den Bemühungen der Web 2.0-Dienstanbieter. Die Rolle des Vertriebskanals tritt in den Hintergrund.

3. Der Nutzer ist als aktiv Mitwirkender in das Geschehen involviert – vom Äußern von Kritik bis hin zur Kooperation bei der Produktgestaltung oder gar der Gelderhebung (Crowdfunding).

4. Plattformen nutzen die sogenannte kollektive Intelligenz. Die prinzipielle Überlegenheit der Schwarmintelligenz ist bislang nicht generell nachgewiesen; sie hat sich dennoch für Massenprodukte als überlegen gezeigt und hat in speziellen Formen auch Einfluss auf komplexe Werterstellung. Als Beispiel kann die Überlegenheit von Wikipedia über klassische und etablierte Enzyklopädien in erstaunlich kurzer Zeit dienen.

5. Individuelle Angebote fördern den Absatz von Nischenprodukten aus dem „Long Tail". Dies erhöht sowohl die Konsumenten- als auch die Produzentenrente.

6. Die Dienste werden über ein Endgerät orchestriert, das nur noch den Zugang zu den Diensten schafft und selbst zwar als Ausgabe für komplexe Dienste dient, sie aber nicht mehr erstellen kann und auf eine Infrastruktur angewiesen ist.

7. Web 2.0 verlangt originelle Nutzerschnittstellen und basiert auf Geschäftsmodellen, die generell als datenzentrisch zu bezeichnen sind.

Der Zugang zu persönlichen Daten ist die Triebfeder dieser Entwicklungen. Die Erhebung der personenbezogenen Daten ist nicht mehr wie noch im E-Commerce ein Nebenprodukt, sondern stellt das ökonomische Ziel des Dienstanbieters dar. Dabei werden vier Szenarien unterschieden:

Personalisierte Web-Dienste sind auf Kunden zugeschnitten und ermöglichen ein direktes Abbild dieses Kunden. Hierbei werden Mining-Verfahren auf Konsumentendaten, zum Beispiel Klickdaten, Suchbegriffe und Browsing-Verhalten, angewandt und zur Musterbildung genutzt.

Online Social Networks (OSN) erheben eine Vielzahl personenbezogener Daten gewissermaßen auf Vorrat und werten sie so aus, dass eine präzise Kategorisierung der Nutzer(muster) möglich ist. Dabei ist es nicht mehr so sehr relevant, dass die Daten einem Nutzer exakt zugeordnet werden können, sondern, dass - im Sinne der Bonitätsermittlung - aussagekräftige Klassen gebildet werden.

Das Cloud Computing als die technische Grundlage des Service Computing erlaubt Computing für alle an einem beliebigen Ort zu niedrigen Preisen, da bei einem aktuellen Überangebot an Computing eine Preiskalkulation auf der Grundlage eines Beitrages zu den Fixkosten gemacht werden kann. Diese kostengünstige und flexible Nutzung von Infrastruktur- und Anwendungsdiensten ermöglicht es, erhebliche Margen aus einem scheinbar unökonomischen - weil kostenfreien - Angebot zu erzielen.

Big Data ist noch von eher wissenschaftlichem oder von infrastrukturellem Interesse. Allerdings gibt es Widerstände bei der Einführung einer Bürgerkarte mit Ausweis-, Arbeits- und Gesundheitsfunktion.[395] Dennoch scheint auch hier ein Wandel in den Gewohnheiten einzutreten.

3.4.1 PERSONALISIERTES WEB

Der Wunsch des Einzelnen nach Unterscheidung und Individualisierung ist ein zentrales Erwerbsmotiv und nimmt in der Werbung und dem Marketing einen wichtigen Platz ein, sodass Daten über Personen von unmittelbarem wirtschaftlichem Wert sind. Personalisierung als Marktanforderung für die Erhebung und Nutzung von Daten im Internet ist ein dreistufiger Prozess.[396] In der ersten Phase soll der Kunde mit seinen Präferenzen und Affinitäten verstanden werden. Dies geschieht durch Datensammlung und Profilbildung. Im Internet werden beispielsweise Klickdaten erhoben, die in aggregierter Form Verhaltensmuster bilden, zum Beispiel typische Klickpfade durch die Katalogstruktur eines Online-Händlers. In der zweiten Phase werden dem Kunden im Rahmen seiner Interaktion mit dem Web personalisierte Angebote unterbreitet; es findet also ein „Matchmaking" zwischen aggregiertem Profilportfolio und aktuellem Kundenprofil und der gegenwärtigen Interaktion statt, woraufhin Angebote kalkuliert und zielgerichtet präsentiert werden. Auf vielen Seiten des Onlineshops von Amazon finden sich zum Beispiel Empfehlungsfenster, die zugeschnitten auf Klickverhalten und Kaufhistorie Produktvorschläge unterbreiten und oft mit einem sprachlichen Zusatz wie „Kunden interessierten sich auch" versehen sind. Hinz und Eckert haben in einer agentenbasierten Simulationsstudie gezeigt, dass der Einsatz solcher „Recommender Systeme" positive Absatzveränderungen bewirken kann, indem gezielt Nischenartikel aus dem „Long Tail" gefördert werden.[397] Des Weiteren bewirken sinkende Suchkosten durch personalisierte Empfehlungen eine steigende Konsumentenrente. Zur Feststellung von Erfolgen wie dem Empfehlungsumsatz und der Konversionsrate, also der tatsächlichen Wirkungskraft der Personalisierungsmaßnahmen, werden daher in einem dritten Schritt Kennzahlen gemessen und, daran ausgerichtet, gegebenenfalls Personalisierungsstrategien angepasst.

Im Rahmen der Bestandsaufnahme gegenwärtiger Nutzungsgrade persönlicher Daten sind Personalisierungsstrategien aber keineswegs auf Internettechnologien beschränkt. Mit dem Einzug von Ubiquitous Computing (UC-) Technologien wie RFID und Sensoren und der Verfügbarkeit von nahezu unsichtbaren, aber doch allgegenwärtigen und spontan vernetzbaren und mobilen Endgeräten in stationären Einkaufsumgebungen, ist Personalisierung im Prinzip überall möglich.[398] So werden in einigen Modell-Supermärkten weltweit Artikelbewegungen über Positionsveränderungen der mit RFID Chips ausgestatteten Artikel erfasst und automatisierte Rückschlüsse über Kaufaffinitäten als Grundlage für personalisierte Angebote durchgeführt. Grundsätzlich wird durch die zunehmende Verbreitung von UC-Technologien die Erhebung von Konsumentendaten „anytime" und „anyplace" vereinfacht. Somit liegt es nahe, in einem zweiten Schritt ubiquitäre Daten auch tatsächlich für Personalisierungsstrategien zu nutzen.

395 Hitachi 2011.
396 Adomavicius / Tuzhilin 2005.
397 Hinz / Eckert 2010.
398 Strüker / Sackmann / Müller 2004.

In Hinblick auf Verletzungen der Privatsphäre durch Personalisierung argumentieren Sackmann, Strüker und Accorsi, dass die Erhebung von Daten nicht länger zu verhindern ist, wenn Kundenverhalten in Zukunft automatisiert dokumentiert und erst in einem zweiten Schritt einzelnen Personen zugeordnet wird.[399] Das Motiv für Personalisierung begünstigt durch Verfahren der automatisierten Dokumentation von Verhaltensweisen, widerspricht somit dem deutschen und europäischen Grundprinzip, möglichst sparsam mit der Erhebung von persönlichen Daten umzugehen.

3.4.2 ONLINE SOCIAL NETWORKS (OSN)

Nach einer aktuellen Umfrage des Branchenverbandes BITKOM führen jüngere Internetnutzer unter 30 Jahren die Mitgliedschaft in sozialen Netzwerken mit einem Anteil von 96 Prozent und deren aktive Nutzung mit 94 Prozent an. Nur rund jeder zweite über 50-Jährige nutzt ein Netzwerk.[400] Facebook ist mit Abstand das populärste Online Social Network (OSN). Die Beweggründe der Nutzung sind vielfältig. So pflegen 73 Prozent darüber Freundschaften, 50 Prozent erhalten Informationen zu Veranstaltungen und 31 Prozent lernen neue Freunde kennen (siehe Abb. 7). Voraussetzung für positive Erfahrungen mit sozialen Netzwerken ist allerdings die umfangreiche Preisgabe persönlicher Daten. Dies schließt eine allgemeine Wertschätzung von Privatsphäre nur scheinbar aus. Facebook-User fassen die Inanspruchnahme des OSN nicht als ein klassisches Tauschgeschäft auf. Ob sie sich der Grundlage des Tausches „persönliche Daten gegen freie Dienste" bewusst sind, ist letztlich eine ungeklärte Frage.

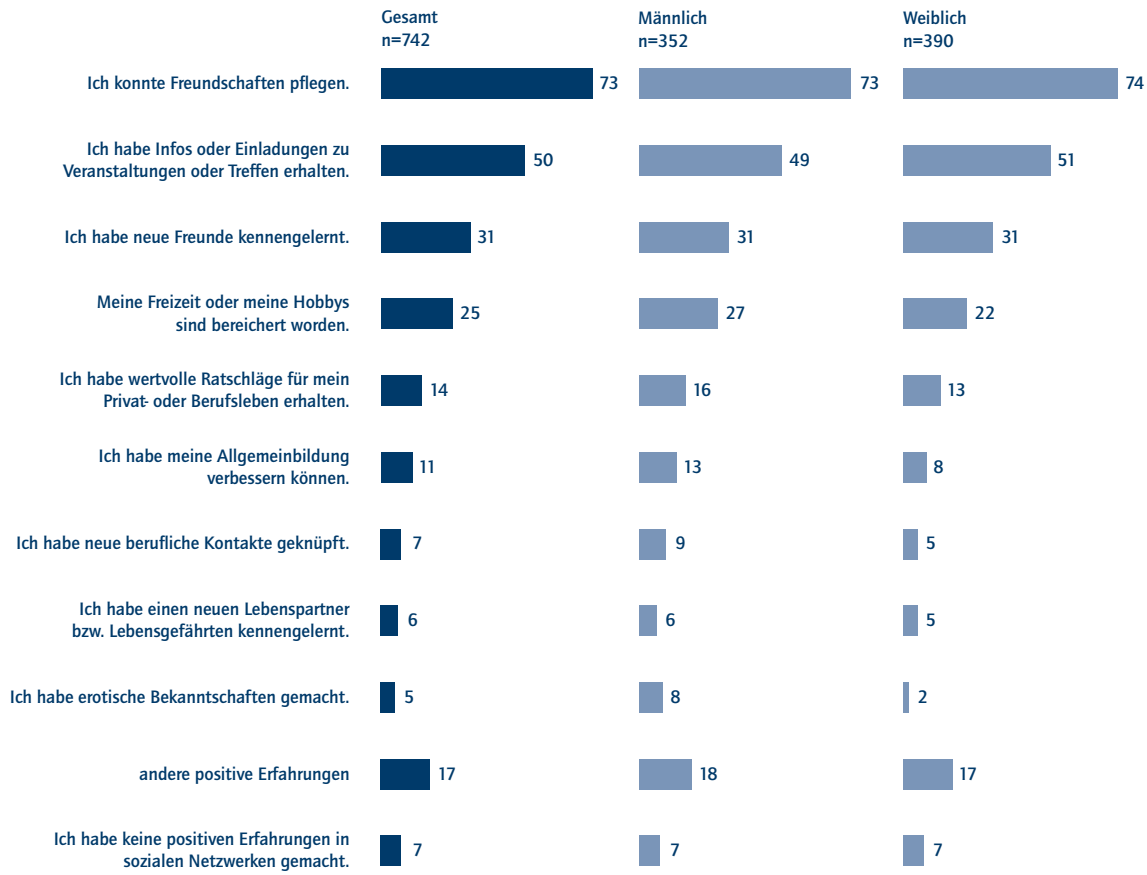
Zu fast allen Profilen zählen der Vor- und Nachname (77 Prozent), das Alter (76 Prozent), ein Portrait-Foto (60 Prozent) und der Beziehungsstatus (57 Prozent). Jeder vierte Nutzer stellt Party- und Urlaubsbilder in ein Netzwerk. Die meisten der gemachten Angaben sind entweder nur für Freunde beziehungsweise eigene Kontakte (41 Prozent) oder sogar nur für bestimmte Freunde (8 Prozent) sichtbar. Der Dienstanbieter hat jedoch immer Zugang. Auffällig ist hier insbesondere die Bereitwilligkeit junger Menschen, ihre persönlichen Daten freizugeben. Man spricht heute gerne von den „Digital Natives", die seit ihrer Kinderstube Mitte der 1990er Jahre mit dem Internet groß geworden sind. Hier ist eindeutig ein unbefangener Umgang mit neuen Medien zu erkennen, vergleicht man Häufigkeit und Art der freigegebenen Daten mit denen älterer Generationen (vgl. Abbildung 8). Die Lebenswelt älterer Menschen über 50 ist weit weniger vom sozialen Umgang im Internet geprägt, was erklärt, dass die Preisgabe von persönlichen Informationen nicht weit über Name und Alter hinausgeht. Die Demografie als Einflussfaktor für Informationsdefizite ist nicht zu vernachlässigen. Geschlechterunterschiede in der Art und Anzahl der veröffentlichten persönlichen Daten von Mitgliedern sozialer Netzwerke sind laut BITKOM-Studie eher gering.

3.4.3 CLOUD COMPUTING

Cloud Computing und Web Services sind die technischen Mittel, um Web 2.0-Dienste wirtschaftlich durchzuführen. Nach einer aktuellen Gartner-Umfrage für das Jahr 2011 ist Cloud Computing die Technologie mit der höchsten Priorität für CIOs,[401] da hier Rationalisierungseffekte als am höchsten erachtet werden. Die Dienste einer Cloud werden dabei in Form von Web Services zur Verfügung gestellt. Damit ist die kombinierte Nutzung von Applikationsdiensten, Anwendungsframeworks und Laufzeitumgebungen verschiedener Dienstanbieter für die Ausführung von Geschäftsprozessen gegeben.[402] Cloud Computing verspricht Kosteneffizienz und Flexibilität, vor allem aber einen unbegrenzten Zugang zu potenziell wirtschaftlich relevanten Diensten. Man lagert

399 Sackmann / Strüker / Accorsi 2006.
400 BITKOM 2011.
401 Gartner 2011a.
402 Müller / Sonehara / Echizen / Wohlgemuth 2011.

Abbildung 7: Positive Erfahrungen in sozialen Netzwerken nach Geschlecht[403]

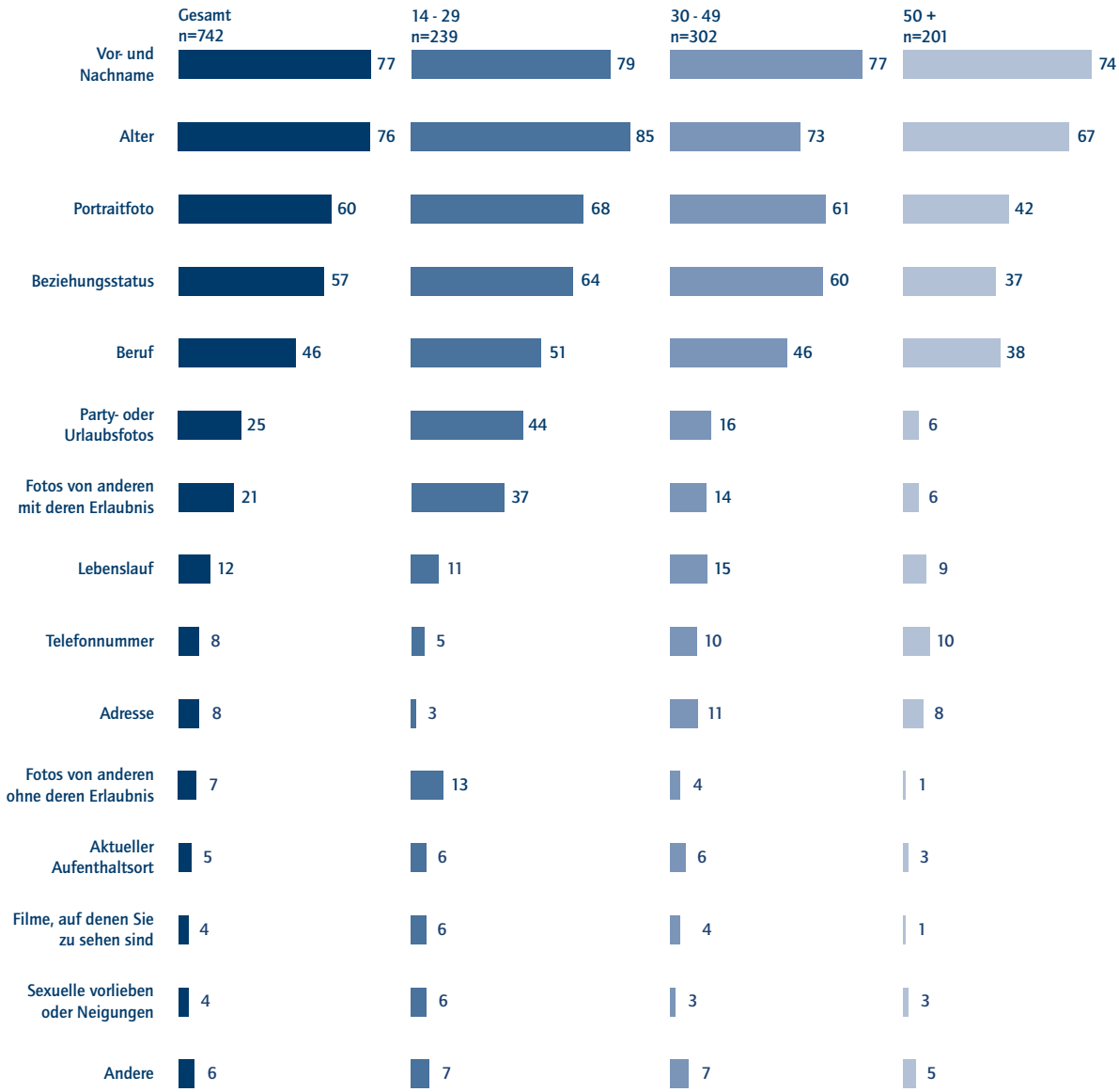


Mehrfachnennungen möglich
Basis: 742 Internetnutzer, die in mind. einem sozialen Netzwerk angemeldet sind.
Frage: "Welche der folgenden positiven Erfahrungen haben Sie bereits in sozialen Netzwerken im Internet gemacht?"
Angaben in Prozent

das Rechnen in eine „Wolke" (Cloud) aus und bezieht von dort die gewünschten Dienste und orchestriert sie zum Beispiel zu höherwertigen Geschäftsprozessen. Im Privaten geschieht dies bereits millionenfach durch die Smartphones, die einen weltweiten Boom erleben. Die Unternehmen werden früher oder später diesem Vorbild folgen. Die Einwände gegen die Cloud werden gegenwärtig noch im Schutz kritischer Daten und in der Aufrechthaltung der Privatheit gesehen. Beides ist mit einem Kontrollverlust verbunden, der durch die Furcht vor wirtschaftlichen Nachteilen begründet wird. Ironischerweise ist ausgerechnet die Branche, die dem Cloud Computing am nächsten steht, am weitesten davon

403 BITKOM 2011.

Abbildung 8: Angaben persönlicher Daten in sozialen Netzwerken nach Alter[404]



Mehrfachnennungen möglich
Basis: 742 Internetnutzer, die in mind. einem sozialen Netzwerk angemeldet sind.
Frage: "Welche der folgenden persönlichen Daten und Infos haben Sie in mindestens einem sozialen Netzwerk angegeben?"
Angaben in Prozent

404 BITKOM 2011.

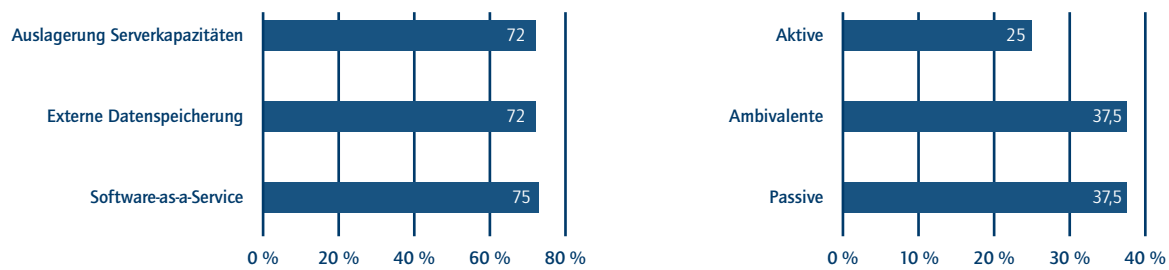
entfernt. Merill Lynch[405] zufolge gibt es bisher nur ein IT-Unternehmen, nämlich die Softwarefirma Salesforce.com, das komplett Cloud-basiert arbeitet. Dieselbe Studie besagt ferner, dass die Top-Fünf-Softwarefirmen (gemessen am Umsatz) nur wenig Gebrauch von der Cloud machen und ihre sensitiven Daten nicht in eine Umgebung auslagern möchten, die sie als nicht zuverlässig und unkontrollierbar einstufen.

Die Notwendigkeit des Cloud Computing zur Aufrechterhaltung von lebensnotwendigen Infrastrukturen erfordert neben der Kontrollfrage zusätzliche Sicherheitseigenschaften. Viele der Sicherheitsanforderungen erscheinen als alter Wein in neuen Schläuchen. Weltweit stellen sich die gleichen Fragen nach Vertrauen in die Einhaltung von Gesetzen und Vereinbarungen sowie um die Gewährleistung einer umfassenden Verfügbarkeit in hoher Qualität. Die Entwicklung von Sicherheitsmechanismen erfolgt unter dem Paradigma des idealen Modells, das heißt, die beteiligten Parteien sind vollständig erfasst und senden ihre Eingaben an eine als vertrauenswürdig definierte dritte Partei, welche die Ergebnisse ohne eigene Interessen berechnet und zurücksendet. Wäre dies in Wirklichkeit der Fall, gäbe es für OSNs keine Geschäftsmodelle.

Laut einer aktuellen Umfrage des Branchenverbandes BITKOM, des Heise Verlages und der HTW Berlin bei mehr als 2000 Händlern und Distributoren zu deren Einstellungen und Erfahrungen mit der Cloud beginnen trotz obiger Anmerkungen Konsumenten und IT-Entscheider mit Vorbereitungen für die Transformation zu Clouds, wobei vor allem das Vermarktungskonzept „Software-as-a-Service" die Neubewertung der Risiken im Vergleich zu den Vorteilen eingeleitet hat (siehe Abb. 9).

Die Mehrheit der befragten Teilnehmer sieht die größten Wachstumschancen in den Bereichen Serverlösungen – also dem reinen Infrastrukturbetrieb in der Cloud (72 Prozent) –, der Auslagerung von Daten (72 Prozent) und dem Betrieb von Anwendungssoftware als Software-as-a-Service (75 Prozent). Lediglich das Aktivitätsniveau der Händler ist noch in den Kinderschuhen. Nur 25 Prozent der Befragten gaben an, ihren Kunden das gesamte Leistungsspektrum des Cloud Computing aktiv anzubieten. 37,5 Prozent der Händler verhalten sich sogar passiv und haben bislang keinerlei Cloud-Leistungen von sich aus angeboten. Der restliche Teil der befragten Teilnehmer verhält sich ambivalent; 37,5 Prozent haben bislang nur vereinzelt Erfahrungen mit der aktiven Vermarktung von Cloud-Lösungen sammeln können.

Abbildung 9: Nachfrageentwicklung und Händleraktivitätsniveau zu Cloud Computing[406]



[405] Chow 2009.
[406] Prüser 2011.

3.4.4 BIG DATA

"Big Data" wird für Datensammlungen benutzt, deren Größe die Bearbeitung mit bekannten Mechanismen, zum Beispiel Datenbanksystemen, verbietet. Gartner sieht "Big Data" als dreidimensionale Struktur. Zum einen sei das Wachstum der Datensammlungen überproportional. Zum zweiten spielt die Geschwindigkeit, mit der die Daten nutzbar gemacht werden können, eine wichtige Rolle. Schließlich ist es die Vielfalt der Datentypen und Datenquellen, die „Big Data" zu einer wirtschaftlich relevanten Größe machen.[407]

Big Data verlangt nach außergewöhnlicher Technologie und hat dadurch noch Kostennachteile. Dennoch haben die Technologien unmittelbare Auswirkungen auf die Privatheit, da mit paralleler Verarbeitung (data mining grids) verteilten Datenbanken und Cloud Computing Plattformen vorhanden sind, die skalierbare Speichersysteme anbieten, handhaben und im Wesentlichen auswerten können.

WalMart verarbeitet die Daten von 1 Million Kunden pro Stunde, Facebook speichert insgesamt etwa 40 Milliarden Fotos mit einem Wachstum von 20 Milliarden Fotos pro Jahr. Dem steht ein enormer technischer Fortschritt gegenüber. Die Decodierung des menschlichen Genoms benötigte vor vier Jahren zehn Jahre, zurzeit kann dies in einer Woche erledigt werden.[408]

Die Kritik an „Big Data" ist interessant, da sie sich weniger auf Privatheit im Sinne von Zugang zu Daten bezieht, sondern auf den Wandel, wie zu Ergebnissen gekommen wird. Nicht mehr die Theoriebildung sei notwendig, sondern allein die Fähigkeit, Daten zu erheben und auf Basis stochastischer Methodik auszuwerten.[409] Die als dritte Einkommensquelle genannten Inferenzen werden damit zum zentralen Gegenstand der Auswertung, die über die Wettbewerbsfähigkeit zukünftiger datenzentrischer Dienste entscheidet. Bei Big Data zeigt sich eine Tendenz zur Trennung von Datensammlung und Datenauswertung. Big Data fokussiert sich auf die Datenauswertung, während gegenwärtige Web 2.0-Dienste noch beide Funktionen ausüben.

In Deutschland ist diese Veränderung der Interpretation von Privatheit vor allem für den Aufbau datenzentrischer Dienste zur Optimierung von Leistungsbezügen wie Pflegeleistungen und ärztlicher Versorgung in der Heterogenität und Ausschließlichkeit der Zielsetzungen darstellbar. Der steigenden Nachfrage nach Gesundheitsleistungen steht ein abnehmendes Arbeitskräftepotenzial gegenüber, das die erforderlichen Leistungen zu erbringen hat.[410] So betrugen die Gesundheitsausgaben der deutschen Krankenversicherungen im Jahr 2008 mehr als 263 Milliarden Euro.[411] Mit „Big Data" könnten die Kostenzunahmen aufgefangen werden.[412] Zum einen könnte die Gesundheitsversorgung auf hohem Niveau standardisiert werden und zum anderen könnte die Diagnose akkurater und kostengünstiger durchgeführt werden.

Große Potenziale dazu bieten die elektronische Gesundheitskarte, elektronische Entgeltleistungen und der elektronische Personalausweis. Alle drei Verfahren ermöglichen dem Anwender, sich auf elektronischem Weg eindeutig zu identifizieren und entsprechende Dienstleistungen in Anspruch zu nehmen. Bei der Nutzung der elektronischen Karten können persönliche Daten des Karteninhabers (beispielsweise die Krankengeschichte oder Beschäftigungszeiten in einem Unternehmen) zentral gespeichert und einer Vielzahl von möglichen Personen zur Verfügung gestellt werden. Die Auswertungen haben Auswirkungen auf die Identifikation von Krankheiten oder Quellen, die zu

407 Gartner 2011b.
408 Webster 2011.
409 Boyd 2010.
410 SVR-Gesundheit 2009.
411 Statistisches Bundesamt 2010
412 Hitachi 2011.

Krankheiten führen. Allerdings sind die aktuellen Spezifikationen nur ein Einstieg in Big Data. Die Gesundheitskarte wird erwähnt, da hiermit eine Technologie bereitsteht, die zurzeit aufgrund von Privatheitsschwachstellen ausgesetzt wird, die jedoch im Rahmen von Big Data und der Idee von statistischen im Gegensatz zu algorithmischen Privatheitsmechanismen zu einer Quelle weitreichender wirtschaftlicher Innovation werden kann.

3.5 ERLÖSQUELLEN DURCH DATENAGGREGATION

Die Erlösquellen von und durch Daten konstituieren sich aus der Nachfrage der Unternehmen, die die datenzentrischen Dienste als Werbeplattform verwenden und gezielt Werbung schalten, um wiederum ihre eigenen Kunden zu erreichen. Die Nutzung von Business Intelligence-Techniken erlaubt die Entdeckung neuer Ableitungen von wirtschaftlich relevanten Zusammenhängen, den Inferenzen. Die datenzentrischen Dienste sind dabei Intermediäre, die nicht unmittelbar selbst aus dem Verhältnis zu ihren Primärkunden Nutzen ziehen. Sie sind jedoch eine Plattform, die eine gezielte Ansprache dieser Primärkunden *in Echtzeit* ermöglicht und erleichtert.

3.5.1 WERBUNG

Mit dem Wandel von Verkäufermärkten zu Käufermärkten Mitte der 1960er Jahre wurde die Werbung zu einem zentralen Erfolgsfaktor unternehmerischen Handelns. Nicht mehr die Notwendigkeit, ein Produkt zu besitzen stand im Mittelpunkt, vielmehr wurden Angebote Ausdruck des Lebensstils der Konsumenten. Die Individualisierung ist seither das wesentliche Verkaufsargument bei festgelegter Produktqualität und Preis. Was bislang durch persönlichen Kontakt und durch Präsentation auf klassischen Werbeträgern wie Papier, Film und Fotographie vonstattenging, wurde seit der Kommerzialisierung des Internets in den späten 1990er Jahren vollständig digitalisiert. Die Online-Werbung übertrifft in Reichweite und Preis-Leistungsverhältnis klassische Printmedien und bietet zusätzlich zu Werbebotschaften die Möglichkeit zur Direktwerbung. Immer leistungsfähigere und nutzerfreundlichere Endgeräte (beispielsweise Smartphones) begünstigen den Erfolg der digitalen Werbewirtschaft, deren Ertragsmodell mit dem der traditionellen Werbewirtschaft konkurriert und dieses heute vielfach übertrifft. Dies lässt sich unter anderem am Rückgang von Zeitungsauflagen erkennen,[413] die durch Werbung finanziert werden. Nach einer aktuellen Online-Befragung von 250 Experten der Werbebranche Ende 2010 legt die Online-Werbung in Deutschland jedes Jahr um mehr als 10 Prozent zu. Die direkte Werbung, bezogen auf den individuellen Kunden, nimmt dabei im Online-Handel die wichtigste Wachstumsposition ein. Obwohl nicht schlüssig und unzweifelhaft bewiesen, erscheint ein Zusammenhang zum Wachstum der sozialen Netze nachvollziehbar und plausibel.[414] Für 2011 sind die Ausgaben deutscher Unternehmen für Werbung im Netz auf rund 3,5 Milliarden Euro geschätzt worden, etwa 16 Prozent mehr als im Vorjahr.[415] Bis 2012 können mehr als 30 Prozent der gesamten Medienzeit auf das stationäre und mobile Internet entfallen. Das Internet könnte somit seinen Anteil am gesamten Werbemarkt von 17 Prozent auf 27 Prozent ausdehnen. Als Wachstumsursache gilt besonders die Verbreitung von mobilen Endgeräten wie Smartphones und Tablet PCs sowie die Akzeptanz internetfähiger Fernsehgeräte. Mehr als 80 Prozent der befragten Experten erwarten ein Zusammenwachsen von Fernsehen und Internet, was weiter für die Nachhaltigkeit des Wachstums der Online-Werbung und dem Verdrängen der übrigen Medien spricht.

Werbeerfolg und -wirksamkeit können gemessen werden und schlagen sich für datenzentrische Dienste in neuartigen

413 Kolo / Meyer-Lucht 2007.
414 FoA 2011a.
415 FAZ 2011b.

Erlösmodellen nieder. Mit der zunehmenden Verfügbarkeit von Klickdaten, die während der Reise durch das Web hinterlassen werden, lassen sich sogenannte performanceorientierte Vergütungsmodelle realisieren. Inzwischen ist der Anteil erfolgsbasierter Vergütungsmodelle bereits auf über 50 Prozent aller Online-Werbekampagnen in Deutschland angestiegen und häufig in Form von Cost-per-Click (CPC), Cost-per-Action (CPA) oder Cost-per-Order (CPO) vorzufinden. Googles CPC-Geschäftsmodell ist beispielsweise für den lukrativen AdWord-Dienst das Ertragsmodell und vergütet Klicks auf Werbelinks. CPA vergütet dagegen nur die auf Klicks folgenden Downloads oder generierten Leads, während CPO den tatsächlichen Verkauf konvertierter Links berücksichtigt. CPC, CPA und CPO lösen zunehmend die sogenannte Reichweiten-orientierte TKP-Vergütung (Tausend Kontakt Preis) ab. TKP-Modelle geben an, welcher Geldbetrag eingesetzt werden muss, um die Reichweite von 1000 Personen einer Zielgruppe per Sichtkontakt zu erreichen.

Laut Expertenbefragung wird die Nutzung von CPC bis 2015 um 3 Prozent leicht ab-, CPO und CPA dagegen um 10 Prozent beziehungsweise 11 Prozent zunehmen.[416] Auch anderen Ertragsmodellen wie Couponing (29 Prozent) oder Revenue Sharing (21 Prozent) wird eine rosige Zukunft vorausgesagt. Der Gutscheinhändler Groupon erhält typischerweise von Anbietern die Hälfte des Wertes eines verkauften Gutscheines. Das Ertragsmodell ist somit erfolgsbasiert. Umsatz wird anteilig an eingereichten Coupons für Produkte oder Dienstleistungen generiert. Dagegen wird beim Revenue Sharing, zum Beispiel bei Apples App Store, Ertrag durch die Beteiligung der Plattform an der Werbung zurechenbaren Umsätzen erwirtschaftet.

Performance-orientierte Ertragsmodelle wie CPC haben den Vorteil, mehr oder weniger in Echtzeit Werbeplätze zu versteigern. Das Realtime Bidding ermöglicht in diesem Kontext die Versteigerung von AdWords in Sekundenbruchteilen, in denen ein Nutzer von einer Seite auf eine andere Seite wechselt. Ist ein Konsument beispielsweise auf der Suche nach Sportartikeln, so können Nike, Adidas und Puma um den attraktivsten Werbeplatz bieten.

Tabelle 5: Dominierte Kanäle durch Vergütungsmodelle[417]

	TV	RADIO	TAGES-ZEITUNG	FACH-PRESSE	AZ-BLÄTTER	AUSSEN-WERBUNG	ONLINE	MOBILE	PUBLIKUMS-ZEITSCHRIFTEN	DIREKT MAILING
Reichweite/ Kontakt (TKP)	89	88	86	84	78	85	40	36	83	47
Couponing	4	6	32	24	30	6	10	21	23	29
Cost-per-Click (CPC)	8	5	7	5	3	2	55	42	5	14
Cost-per-Action (CPA)	10	13	11	10	5	10	46	44	9	37
Cost-per-Order (CPO)	15	7	9	11	10	4	58	49	5	45
Revenue Sharing	22	18	14	12	7	5	20	20	13	12

416 FoA 2011.
417 FoA 2011.

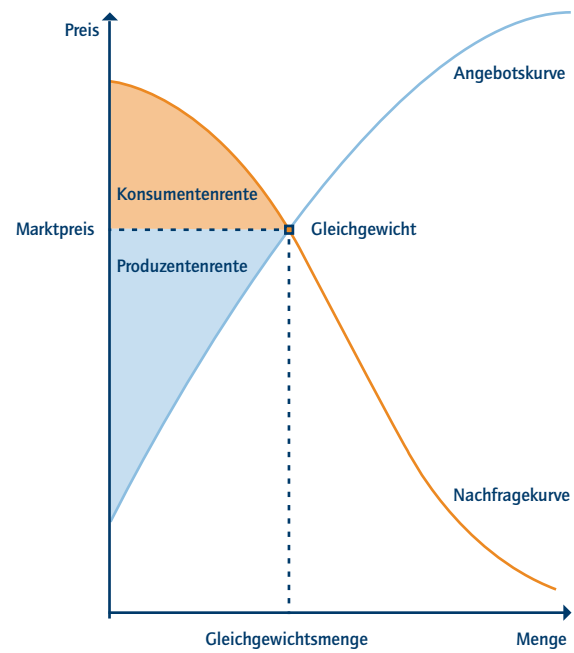
3.5.2 PREISDIFFERENZIERUNG

Datenzentrische Dienste liefern Informationen zu Dienstleistungen und Waren, die für große Nachfrageschichten als nicht erreichbar galten. Man könnte diese Waren und Dienstleistungen als „verborgen" klassifizieren und die Aufdeckung ihrer Erwerbbarkeit durch eine größere als bisher geglaubte Käuferschicht, zum Beispiel durch einen deutlich unter den üblichen Angeboten liegenden Preis als Rationalisierungsbeitrag der datenzentrischen Dienste bezeichnen. Man nennt diese Werte auch „intangible assets", die sich durch die Unmöglichkeit auszeichnen, in traditionellen Wertschöpfungsmetriken wie Bilanzen oder Gewinn- und Verlustrechnungen registriert zu werden. Dementsprechend finden sich solche Beiträge von Suchanfragen im Internet auch nicht in Statistiken wie dem Bruttoinlandsprodukt (BIP).[418] Nichtsdestotrotz bietet die Internetökonomie Instrumente zu Quantifizierung und Abschätzung der Werte, die im Wesentlichen durch eine akzeptierte Preisdifferenzierung generiert wird.[419] Wenn der Anbieter die Zahlungsbereitschaft des Nutzers kennt, dann kann bei Verfügbarkeit oder Überschuss an Waren ein dafür passender Preis definiert werden. Erfolgt ein solches Angebot nach Befriedigung des Primärmarktes, ist die zeitliche Verlagerung eine akzeptierbare Form der Preisdifferenzierung durch ein ansonsten transparentes Medium.

Die Konsumentenrente (consumer surplus) ist der aggregierte Nutzen, den Konsumenten durch die Inanspruchnahme einer Leistung beziehungsweise dem Verbrauch eines Gutes nach Abzug des Preises (market price) erhalten (vgl. Abb. 10). Gleichgewichtspreis und Gleichgewichtsmenge (equilibrium quantity) ergeben sich dort, wo die Nachfrage gleich dem Angebot ist. Die Fläche zwischen der abfallenden Nachfragekurve (demand curve) und dem Gleichgewichtspreis (equilibrium price) entspricht der Konsumentenrente. Die Produzentenrente (producer surplus) entspricht der Fläche oberhalb der Angebotskurve (supply curve) und unterhalb des Gleichgewichtspreises. Ein Konsument erzielt also dann eine Rente, wenn er die Ware zu einem Preis erwerben kann, der geringer als seine Zahlungsbereitschaft ist. Ebenso erzielt der Anbieter einen Vorteil, wenn der Marktpreis höher als sein Reservationspreis ist. Datenzentrische Dienste haben den Umgang mit Preisen nicht erfunden, aber sie haben ihn durch die Datenaggregation global ermöglicht.

Eine der ersten Studien zur Abschätzung der Konsumentenrente im Internet wurde 2003 von Brynjolfsson, Smith und Hu durchgeführt.[420] Die Autoren konnten zeigen, dass Konsumenten im Internetbuchhandel allein durch die Varietät an Angeboten – im Gegensatz zu niedrigeren Preisen – eine Konsumentenrente von 1 Milliarde zusteht.

Abbildung 10: Konsumentenrente und Produzentenrente



418 Brynjolfsson / Saunders 2010.
419 Varian 2011.
420 Brynjolfsson / Smith / Hu 2003.

Bapna, Jank und Shmueli haben die Konsumentenrente durch Transaktionen auf eBay geschätzt und herausgefunden, dass die mittlere Rente mindestens 4 US-Dollar pro Auktion entspricht und im Jahr 2003 einem Wert von etwa 7 Milliarden US-Dollar ausmachte.[421]

Ähnliche Jahreswerte ermittelten Goolsbee und Petrin für die Einführung eines Satelliten-Rundfunkdienstes.[422] Die Summe der Konsumentenrente ergab sich aus dem Nutzen für Anwender der Satellitentechnologie und dem Nutzen für Kunden von Kabelanschlüssen. Letztere konnten trotz Einführung des Satellitenrundfunks immer noch von geringeren Preisen und einer höherer Qualität profitieren und somit eine höhere Konsumentenrente einstreichen.

Ghose, Smith, Telang untersuchten den Buchmarkt auf *amazon.com* und zeigten, dass die meisten Verkäufe von gebrauchten Büchern keine Kannibalisierung der Verkäufe neuer Bücher zur Folge hatte und somit die Wohlfahrt des gesamten Buchmarktes gesteigert werden kann. Die Konsumentenrente der Kunden gebrauchter Bücher erfährt ebenfalls einen Zuwachs und wird auf annähernd 67 Millionen US-Dollar geschätzt.[423]

3.5.3 INFERENZEN

Das Bilden von Inferenzen, also das Ableiten von Zusammenhängen aus vorliegenden Daten, ist ein neues und das bislang am wenigsten entwickelte Erwerbsfeld datenzentrischer Dienste. Geschäftlich ermöglicht wird eine solche Fähigkeit zum einen durch die Ko-Evolution von Technik und Analysefähigkeiten. Die Methoden des Business Intelligence (oder deutsch Geschäftsaufklärung) erlauben die Gewinnung von Erkenntnissen, die in Hinsicht auf die Unternehmensziele bessere operative oder strategische Entscheidungen ermöglichen. Der Begriff „Intelligence" bezeichnet die aus dem Sammeln und Aufbereiten erworbener Informationen gewonnenen Erkenntnisse. Diese Fähigkeiten und die komparativen Vorteile der datenzentrischen Dienste für ihre Anwendung sind durch vier Merkmale gekennzeichnet:

a) Globale Orientierung und generelle, nicht produktorientierte Datensammlung,
b) Überlegene Auswertungsmöglichkeiten,
c) Zusammenführung von Daten und Wissen mit der aktuellen Interaktion der Nutzer,
d) Permanente Verbesserung und Vergrößerung der Datenbasis in Abhängigkeit von der Attraktivität der Dienste.

Neben der Inferenzbildung werden in experimentellen Innovationen nicht nur aktuelle Zusammenhänge aufgezeigt, sondern Prognosen in Hinblick auf zukünftige Entwicklungen durchgeführt. Die Grundlage für Erlösmodelle der datenzentrischen Dienste erfolgt in einem dreistufigen Prozess: (1) Die Datenerfassung durch attraktive Dienste, (2) die Herstellung eines Zusammenhanges, sodass Muster und Diskontinuitäten sichtbar werden und (3) in der letzten Stufe die Bereitstellung der aufbereiteten Daten an Nachfrager, meist auf der Plattform des Dienstes. Insbesondere in der zweiten Stufe sind weitere Fortschritte in der Analysetechnik und in der Datenaggregation und Zusammenführung zu erwarten, wenn datenzentrische Dienste zum Beispiel durch Zukäufe spezialisierter Dienste ihre Datenbasis erweitern.

Inferenzen und Business Intelligence-Verfahren datenzentrischer Dienste und deren Anwendung stellen meist ein geschäftsdefinierendes Geheimnis dar. Ihr Umfang kann nur indirekt abgeschätzt werden. Gegenwärtig wächst in Deutschland der Markt der BI-Analysen um jährlich 8 Prozent und wurde für 2009 auf insgesamt 816 Millionen Euro

421 Bapna / Jank / Shmueli 2008.
422 Goolsbee / Petrin 2004.
423 Ghose / Smith / Telang 2006.

geschätzt. Seither ist eine zunehmende Konzentration auf wenige Anbieter festzustellen, die insgesamt 61 Prozent des BI-Marktes unter sich aufteilen.[424]

3.5.4 KOMMERZIELLE ENTWICKLUNG

Google hat mit seiner Suchmaschine bereits einen Anteil am Online-Werbemarkt von rund 60 Prozent. Facebook wird nach Branchenexperten im Jahr 2011 in Deutschland einen Online-Werbeumsatz von 200 Millionen Euro erzielen und sich damit vor den drei großen Online-Vermarktern Interactive Media, Tomorrow Focus und United Internet positionieren. Im internationalen Vergleich liegen rund drei Viertel des gesamten Marktes in der Hand von Branchengrößen wie Google, Facebook, Microsoft, Yahoo und eBay.

Für das soziale Netzwerk Facebook wurde im Jahr 2011 (Stand: September 2011) ein Werbeumsatz von 3,8 Milliarden US-Dollar und ein Gewinn von 1 Milliarde US-Dollar prognostiziert.[425] Hier gelten persönliche Empfehlungen von den eigenen Kontakten als wirksamste Werbebotschaft. 2,1 Milliarden US-Dollar sind dem Werbeumsatz in den Vereinigten Staaten zuzurechnen. Facebook ist damit in den USA Marktführer im Geschäft mit Online-Werbung, dicht gefolgt von Google, Yahoo und Microsoft.

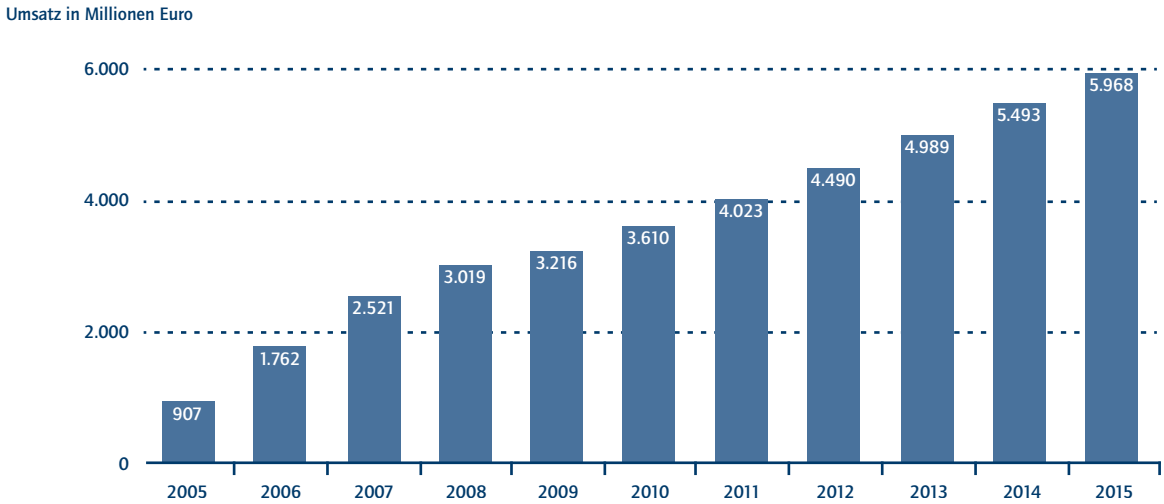
Im Gegensatz zu Facebook und Google sind Online Marketing-Agenturen wie Interactive Media und Tomorrow Focus in erster Linie Anbieter von (digitalen) Inhalten (zum Beispiel News) oder Dienstleistungen (zum Beispiel Partnervermittlung) und somit dem Web 2.0 in direkter Form nicht zuzurechnen. Gleichzeitig werden aber Inhalte und Dienstleistungen frei zur Verfügung gestellt und Erträge mit Online-Werbung und Datenhandel erwirtschaftet. Neben der Online-Werbung bietet die Erhebung und Verwertung von Daten aber auch andere Potenziale zur Leistungssteigerung von Unternehmen.

Tabelle 6: AGOF Online-Vermarkter in Deutschland nach Reichweite[426]

ONLINE MARKETING AGENTUREN	TOP WEBSEITEN	REICHWEITE (Q2 2010) IN % DER INTERNET USER	# IN MIO. BESUCHER DER WEBSEITE
InteractiveMedia CCSP	T-Online, RTL2	63,5	31,53
TOMORROW FOCUS	Focus, Playboy, Chip	60,4	30,03
SevenOne Media	MyVideo, icq, N24	53,5	26,59
United Internet AG	WEB.DE, GMX, 1&1	51,9	25,79
IP Deutschland	WKW, StayFriends, Sky	50,5	25,09
eBay Advertising Group	eBay	49,2	24,47
Yahoo! Deutschland	Yahoo!, Eurosport, Flickr	47,2	23,47
Axel Springer Media Impact	Bild, Welt, RollingStone	45,9	22,80
Ströer Interactive	MySpace, immonet, idealo	44,4	22,06
Microsoft Advertising	MSN, Massive	44,3	22,02

424 Apel 2009.
425 FAZ 2011a.
426 FoA 2011.

Abbildung 11: Umsätze mit Online-Werbung in Deutschland[427]



Brynjolfsson, Hitt, Lorin und Kim untersuchen die Auswirkungen von datenbasierten Entscheidungen auf die Leistungsfähigkeit von Unternehmen.[428] Eine Befragung von 179 Großunternehmen zu ihren Geschäftsprozessen und IT-Investitionen ergab eine durchschnittliche Steigerung der Produktivität zwischen 5 Prozent und 6 Prozent im Vergleich zur Produktivität, die mit sonstigen Investitionen und sonstiger IT-Nutzung erwartet wurde. Ausgangssituation der Studie ist die Prävalenz von Business Intelligence-Methoden, die mittels Verfahren zur Datenanalyse große Mengen an Unternehmensdaten zur Entscheidungsunterstützung mit Mehrwert versehen. Somit haben Unternehmen mittels Data Mining-Verfahren die Möglichkeit, Geschäftsideen vor ihrer Umsetzung einem Test zu unterziehen und je nach Testergebnis die Transformation ihres Geschäftsmodells auf Basis einer „information-based strategy"[429] voranzutreiben.

3.6 NUTZERVERHALTEN

Wie verhalten sich Nutzer angesichts der Gefahr der Offenlegung ihrer persönlichen Daten? Von wirtschaftlicher Relevanz in dem hier verfolgten Bezugsrahmen ist die Frage, ob das Signalisieren von Privatheitseigenschaften für zu handelnde Produkte die Geschäftstätigkeit fördert. Prinzipiell ist die informationelle Selbstbestimmung als Prinzip deutscher und europäischer Gesetzgebung ein der Marktwirtschaft angepasstes Gesetz, da es scheinbar die individuelle Freiheit und Entscheidungsmacht unterstützt. Westin hat Privatheit einleuchtend beschrieben: „Privacy is the claim of individuals, groups or institutions to determine for themselves when, how, and to what extent information about them is communicated to others".[430] Die Voraussetzung, dieses Prinzip für den Einzelnen im Internet nicht zu einem bloßen Ideal, sondern zur Realität werden zu lassen, ist an drei Bedingungen gebunden:

427 Statista 2011.
428 Brynjolfsson / Hitt / Kim 2011.
429 Davenport 2009.
430 Westin 1967.

(1) Es erfordert die Wirksamkeit und Verfügbarkeit von Sicherheitsmechanismen, worunter die Garantie zur Einhaltung von Schutzzielen verstanden werden muss, die in freien und gleichberechtigten Verhandlungen zwischen den Marktteilnehmern festgelegt werden können.
(2) Vertrauensbildende Maßnahmen, wie zum Beispiel PKI-Infrastrukturen, sind die Vertrauensplattform, auf der individuelle Vereinbarungen erfolgen und die von der Infrastruktur garantiert werden.
(3) Die Komplexität zyklischer Transaktionen muss für die Marktteilnehmer nachvollziehbar sein und es muss die Fähigkeit zur Auswahl der geeigneten Sicherheitsverfahren vorhanden sein. Insgesamt zeigt eine Vielzahl von Studien, unter anderem die Freiburger Studie aus dem Jahre 2003, dass sich zwar ein Drittel der damaligen Probanden als Sicherheitsexperten eingeschätzt hat, diese aber bei Versuchen kaum weniger sicherheitsrelevante Fehler begangen haben als die sogenannten aufgeklärten Laien oder gar die wirklichen Sicherheitslaien. Den potenziellen Nutzen der persönlichen Daten für andere und den bei den Probanden aufgetretenen Schaden durch Sicherheitslücken konnte niemand einschätzen.[431]

Nachfolgend werden drei Prinzipien zur Erklärung der Nutzerverhaltens vorgestellt, die sich in einer Welt zurechtfinden sollen, die durch die obigen drei Bedingungen skizziert ist:

3.6.1 DAS PRIVACY PARADOX

Bei Untersuchungen zum Verhalten von Anwendern kristallisiert sich immer wieder heraus, dass zwar eine erhöhte Aufmerksamkeit bezüglich Datenmissbrauch vorhanden ist, dies allein jedoch das Verhalten der Mehrheit wenig beeinflusst. Dies wird als *Privacy Paradox* bezeichnet und ist von Acquisti und Grossklags erstmals so benannt und auch empirisch belegt worden.[432] Varian zeigt, dass private Akteure einerseits dem Schutz der Privatheit eine hohe Wertschätzung zuerkennen, jedoch andererseits in konkreten Entscheidungssituationen sehr freigiebig persönliche Daten anbieten.[433] Bislang gibt es zwar zahlreiche kasuistisch nachgewiesene Evidenzen,[434] aber theoriebegründete Modelle zur Erklärung dieses Phänomens fehlen.[435] Allerdings fehlen auch geschlossene Theorien zur Wirkung der Regulierung des Datenschutzes auf wirtschaftliches Handeln. Marc Zuckerberg von Facebook und Eric Schmidt von Google halten den Datenschutz und die Privatheit für ein *Auslaufmodell*.[436] Ein Ausgleich der Interessen ist zum Beispiel über die Ökonomisierung des Datenschutzes möglich, indem man Eigentumsrechte vergibt. Dies ist Gegenstand einer in den USA entstehenden und in Europa eher nachhinkenden Diskussion zur Anpassung des Datenschutzes an die technische Entwicklung.[437]

Zahlreiche Autoren erklären das Privacy Paradox mit ökonomisch irrationalem Verhalten, da die Nutzer scheinbar wider besseres Wissen keine optimale Kosten-Nutzen-Relation wählen. Das Paradox, also die Diskrepanz zwischen Privacy-Einstellung und tatsächlichem Verhalten, erklären andere Autoren mit der Kontextabhängigkeit der jeweiligen Entscheidungssituation. Die Abweichung zwischen Wertschätzung persönlicher Daten und tatsächlichem Offenbarungsverhalten ergibt sich aufgrund der Inkompatibilität der jeweiligen Entscheidungssituation zueinander. Während Privatheit als allgemeines Prinzip sehr hoch eingeschätzt wird, erfolgt immer dann eine Relativierung, wenn eine konkrete Transaktion bevorsteht.

431 Kaiser / Reichenbach 2002.
432 Acquisti / Grossklags 2003.
433 Varian 1996.
434 Berendt / Günther / Spiekermann 2005.
435 Acquisti / Grossklags 2007.
436 Müller 2010b
437 Müller 2010a.

Die möglichen Konsequenzen, das heißt der potenzielle Nutzen und die möglichen Risiken, sind nicht determiniert (Indeterminiertheit). Ferner ist es möglich, dass der Aufbau der Befragungen einen Einfluss auf die Ergebnisse hat, wobei immer zuerst nach der allgemeinen Wertschätzung von Privatheit gefragt wird, ehe diese für eine Entscheidungssituation konkretisiert und dadurch relativiert wird (Nicht-Kommutativität).[438] Auch Acquisti vertritt die Ansicht, dass dieses scheinbar paradoxe Verhalten nicht als Irrationalität seitens der Kunden gelten kann, sondern auf den Einfluss verschiedener Faktoren, wie inkonsistente Präferenzen, gegenläufige Bedürfnissen, unvollständigen Informationen über mögliche Risiken, begrenzte kognitive Fähigkeiten sowie unterschiedliche systematische Abweichungen vom abstrakten rationalen Entscheidungsprozess zurückzuführen ist.[439]

3.6.2 RATIONALITÄT DURCH SCHULUNG

Datensparsamkeit ist das grundlegende Prinzip der informationellen Selbstbestimmung. Sie bedeutet, dass man nichts an Daten preisgeben sollte, wenn die Kenntnis der Daten nicht in Zusammenhang mit einer gewünschten Transaktion steht. Ergebnisse von Studien zeigen, dass von Nutzern meist bereitwillig zu viele Daten angegeben werden und andererseits von den datenzentrischen Diensten auch Auskünfte gefordert werden, die offensichtlich nichts zum Zweck der Transaktion beitragen.[440] Eine oft vertretene Erklärung eines solchen Verhaltens ist die mangelnde Aufklärung und Schulung der Nutzer. Mit Hilfe von PET-Mechanismen könne dann Datensparsamkeit realisiert werden und so die informationelle Selbstbestimmung zur faktischen Wirklichkeit werden.[441]

Whitten und Tygar untersuchen in diesem Kontext das Sicherheitswerkzeug PGP 5.0 und zeigen, dass dieses durch Normalbenutzer nicht beziehungsweise nur unzureichend bedienbar ist und dadurch nur zur Unsicherheit beiträgt, ja sogar dazu verleitet, dass dieser sich in Scheinsicherheit wägt.[442] Eine Studie aus Freiburg präzisiert die Untersuchungen zur Wirksamkeit von Schulungen und Nutzbarkeit. Mit dem Ziel, eine Metrik für die Nutzbarkeit eines Sicherheitsmechanismus zu entwickeln, befassen sich Kaiser und Reichenbach.[443] Sie klassifizieren Fehler, die im Zusammenhang mit der Nutzung von Sicherheitsmechanismen am häufigsten gemacht werden. Dabei unterscheiden sie vier Sicherheitsklassen:

Problemklasse I umfasst die nicht sicherheitskritischen Benutzerprobleme, während Problemklasse IV die systemimmanenten Sicherheitsprobleme erfasst. Die Schnittmenge dieser beiden Klassen umfasst die sicherheitskritischen Benutzerinteraktionen, durch die die Schutzziele Vertraulichkeit, Integrität, Zurechenbarkeit als auch Verfügbarkeit gefährdet werden können. Beachtet man nun die Sicherheitskompetenz, ergeben sich zwei Verhaltensmuster: In der Problemklasse II sind solche Benutzer erfasst, die sicherheitskritische Interaktionen durchführen und Sicherheitskompetenz nachgewiesen haben, während Problemklasse III die sicherheitskritischen Benutzbarkeitsprobleme aufgrund mangelnder Sicherheitskompetenz enthält. Aufbauend auf dieser Klassifikation wurden anhand von Laborexperimenten in Zusammenarbeit mit der deutschen Post die beschriebenen Problemklassen bzgl. der Schutzziele im E-Commerce empirisch untersucht. Dabei zeigt sich, dass 75 Prozent aller Nennungen der 120 befragten Personen sich den sicherheitskritischen Benutzbarkeitsproblemen zuordnen lassen und die Mechanismen somit gar nicht oder fehlerhaft genutzt werden. Die Nutzbarkeit von Sicherheitswerkzeugen zeigt sich somit als die hauptsächliche Ursache für sicherheitskritische Vorfälle.

438 Flender / Müller 2012.
439 Acquisti 2009.
440 Acquisti 2009.
441 Müller 2008.
442 Whitten / Tygar 1999.
443 Kaiser / Reichenbach 2002.

Kaiser untersucht mittels einer zweiten empirischen Studie, warum heutige Internetnutzer Sicherheitsmechanismen in IT-Anwendungen nicht oder nur eingeschränkt nutzen.[444] Hierzu fand sowohl eine schriftliche als auch eine Online-Befragung von zufällig ausgewählten Internet- und E-Mail-Nutzern statt. Die Befragung beinhaltet neben persönlichen Daten und den Vorkenntnissen in Internet und Sicherheit das Sicherheitsbewusstsein, die Zahlungsbereitschaft für Sicherheitsmechanismen als auch das Sicherheitsverständnis. Anhand der Antworten von 876 Befragten werden mittels Punktevergabe Endverbraucher nach Sicherheitsbezug klassifiziert:

Tabelle 7: Nutzergruppen klassifiziert nach Sicherheitsbezug

NUTZERGRUPPE	ANZAHL
Sicherheitsexperten	5
Fortgeschrittene	249
Sicherheitslaien	622

Die Gruppe der Sicherheitslaien ist dabei am stärksten repräsentiert.[445] In einem nächsten Schritt wird diese Klasse anhand der Kriterien Nutzungshäufigkeit von Sicherheitskonzepten, Sicherheitskenntnissen, Einschätzung der Sicherheitsgefahren als auch Lern- und Zahlungsbereitschaft genauer analysiert. Alle Nutzer waren unabhängig von ihrer Selbsteinschätzung der Laiengruppe zuzuordnen. Danach existieren innerhalb dieser objektiven Sicherheitslaien unterschiedliche Ausprägungen. Kaiser leitet resultierend drei Subklassen ab, die sich durch folgende spezifische Merkmale unterscheiden:

- Sicherheitslaie 1 (SL 1): „Die gefährdeten Gutgläubigen"
- Sicherheitslaie 2 (SL 2): „Die gutgläubigen Bereitwilligen"
- Sicherheitslaie 3 (SL 3): „Die selbstbewussten Könner"

Mit 65 Prozent der Gesamtklasse ist die Gruppe SL 1 am stärksten vertreten; sie zeichnet sich durch äußerst geringe Lernwilligkeit und Gefährdungswahrnehmung aus. Rund 20 Prozent der Laien befinden sich in der Klasse SL 2, die Sicherheitsgefahren als teilweise wahrscheinlich, teilweise eher unwahrscheinlich einstufen und Sicherheitsmechanismen nur bei sofortiger Verständlichkeit einsetzten. Häufige Internetnutzung, häufiger Einsatz von Sicherheitsmechanismen sowie eine sehr geringe Zahlungsbereitschaft zeichnet die Klasse SL 3 aus, die als Laien zu bezeichnen sind und ca. 15 Prozent umfassen. Die Schulung des Sicherheitsbewusstseins und die Sensibilisierung zur sicherheitskritischen Handhabung der Mechanismen verhindern in allen Studien kaum Fehlverhalten.

3.6.3 VERHALTENSDETERMINIERTE RATIONALITÄT

Wenn weder Rationalität noch Schulung zur Erlangung von Rationalität zum generellen Einsatz von PET führt, erklärt die verhaltensbasierte Wirtschaftstheorie den zu beobachtenden Verzicht auf Privatheitsvorkehrungen als Ausprägung von grundlegenden Verhaltensnormen. Sie beschäftigt sich mit menschlichem Verhalten in wirtschaftlichen Situationen. Dabei werden Konstellationen untersucht, in denen Menschen im Widerspruch zur Modell-Annahme eines rationalen Nutzenmaximierers agieren.

Culnan und Armstrong analysierten eine zwischen 1990 und 1994 erhobene Studie von Louis Harris über die Haltung von Konsumenten bezüglich Privatheitsfragen, um eine detaillierte Klassifikation der beobachteten Verhaltensweisen zu schaffen und unterscheiden resultierend zwischen (a) der Angst eines unauthorisierten Zugriffs aufgrund von Sicherheitslücken beziehungsweise dem Mangel an internen Kontrollen sowie (b) der Sorge vor einer missbräuchlichen, nicht zweckgebundenen (Weiter-)Verwendung der Daten wie der Weitergabe an

444 Kaiser 2003.
445 Kaiser / Reichenbach 2002.

Dritte.[446] Die ursprünglich von Harris durchgeführte Studie basiert auf der Erhebung von 1000 Telefoninterviews mit zufällig ausgewählten volljährigen Personen der US-Bevölkerung.[447] Mittels einer breiten Meta-Analyse von Privatheit betreffenden Studien können Smith, Milberg und Burke zusätzlich (c) die generelle Sorge um Datensammlung sowie (d) die Angst vor möglicher Unfähigkeit zur Berichtigung von Fehlern identifizieren.[448] Somit lässt sich belegen, dass der Entscheidung zur Datenpreisgabe und dem hieraus entstehen Nutzen eine Wahrnehmung von möglichen Risiken und demzufolge Kosten seitens der Endverbraucher gegenübersteht.

Wie empirische Untersuchungen weiterhin darlegen, variiert die Einschätzung dieser Risiken jedoch stark mit Bezug zum jeweiligen Individuum. Berendt, Günther und Spiekermann verdeutlichen dies mittels eines Laborexperiments mit 206 Probanden, deren Online Shopping-Verhalten untersucht wurde.[449] Durch die Beantwortung eines Fragebogens wird die latente Bereitschaft der Probanden zur Herausgabe persönlicher Informationen abgefragt und analysiert. Gegenstand der Befragung ist neben der Bereitschaft zur Preisgabe von persönlichen Daten die individuelle Wertung der Privatheit. Die Autoren zeigen, dass sich Endverbraucher bezüglich der Ausprägung ihrer Privatheitsinteressen in drei Klassen unterteilen lassen: (1) Den „marginally concerned" (24 Prozent), die sich durch Gleichgültigkeit bzgl. Ihrer Privatheit auszeichnen; (2) den „Privacy-Fundamentalists" (30 Prozent), die enormen Wert auf die Wahrung ihrer Privatheit legen sowie (3) der „pragmatic majority", die einerseits das Interesse verfolgt, ihre Privatheit zu wahren, diese aber andererseits für die Erlangung eines Nutzens bereit ist aufzugeben. Letzte Gruppe wird wiederum in die Subklassen (3.1) „identity concerned user" (20 Prozent), die sich mehr über die Offenbarung von persönlichen Informationen wie Name oder Adresse sorgen, und (3.2) „profile averse user" (26 Prozent), die die Preisgabe von Informationen wie Interessen, Hobbies oder der Gesundheit meiden, unterteilt. Studien von Kumaraguru und Cranor sowie Ackerman et al. zeigen konsistente Ergebnisse.[450, 451]

Somit werden Informationen über gewisse Lebensbereiche personenspezifisch privater als andere bewertet. In konkreten Entscheidungssituationen bedeutet dies, dass Endverbraucher, die ein hohes Interesse an der Wahrung ihrer Privatheit aufweisen, der Datenpreisgabe einen wesentlich höheren Wert zuweisen als Personen, die weniger Privatheitsängste aufweisen. Weiterhin wird deutlich, dass die Art der preiszugebenden Information und deren Wertung das Verhalten beeinflussen: Für „identity concerned user" beispielweise ist die Preisgabe von Hobbies und Interessen mit einem niedrigeren Risiko und hieraus folgend einem niedrigeren Kostenfaktor behaftet als für „profile averse user", welche die Preisgabe dieser Informationen scheuen. Privatheit ist für die Nutzer ein handelbares Gut, für dessen Aufgabe ein Vorteil – ob monetärer Art oder durch Zugang zu speziellen Diensten und Services – ermöglicht wird. Es wird allerdings auch hier die Fähigkeit zur rationalen Entscheidung auf Basis vollständiger Information unterstellt.

Einen anderen Schwerpunkt in der Untersuchung der ökonomischen Aspekte der Privatheit zeigt Varian, indem er einen Markt für Informationen betrachtet, an welchem Datenanbieter Informationen an Datenkonsumenten preisgeben oder schützen.[452] Die den ökonomischen Modellen zugrunde liegende Annahme der stabilen Präferenzen ist

446 Culnan / Armnstrong 1999.
447 Harris 1994.
448 Smith / Milberg / Burke 1996.
449 Berendt / Günther / Spiekermann 2005.
450 Kumaraguru / Cranor 2005.
451 Ackermann / Cranor / Reagle 1999.
452 Varian 1996.

jedoch zu restriktiv und missachtet die psychologischen und emotionalen Komponenten der Privatheit betreffenden Entscheidungen.[453] Das hieraus resultierende Forschungsgebiet der verhaltensorientierten Ökonomie befasst sich nun mit informationellen Trade-Offs: Es wird untersucht, was die ausschlaggebenden Faktoren sind, spezielle Daten in einem spezifischen Kontext preiszugeben oder zu schützen.

Grossklags und Acquisti untersuchen einerseits die Bereitwilligkeit, für den Schutz von persönlichen Daten zu zahlen sowie andererseits die Bereitwilligkeit, diese gegen monetäre Gegenleistung zu veräußern.[454] Zu diesem Zweck führen sie ein Probandenexperiment mit 47 Teilnehmern durch. In einem ersten Teil wird ein Quiz durchgeführt, dessen Ergebnis aufgezeichnet wird. Zusätzlich werden persönliche Daten der Probanden (Gewicht, Urlaubspräferenzen, Anzahl Sexualpartner) mittels eines Fragebogens erhoben. Im zweiten Teil stehen die Probanden vor der Entscheidung, ihre im Fragebogen angegebenen Antworten sowie ihr Quizergebnis gegen Bezahlung entweder zu schützen oder aber gegen Vergütung allen Teilnehmern preiszugeben. Als Resultat zeigt sich, dass unabhängig von der Sensitivität der Information, die Bereitschaft, diese gegen Vergütung preiszugeben wesentlich höher eingestuft werden kann, als die Bereitschaft diese Information gegen anfallende Kosten zu schützen. Allerdings bleibt der Fakt ersichtlich, dass gewisse Informationen, wie beispielweise das Körpergewicht, mit einem wesentlich höheren Preis (31,8 US-Dollar) durchschnittlich bewertet werden als andere (Urlaubspräferenzen 6 US-Dollar im Mittel). Die hohen Standardabweichungen der berechneten Mittelwerte (148 US-Dollar bei Gewicht; 16,7 US-Dollar bei Urlaubspräferenz) verdeutlich zudem, wie unterschiedlich Personen eine Information in Bezug auf deren Privatheitsaspekt bewerten.

Beresford, Kübler und Preibusch zeigen dazu vergleichbare Ergebnisse.[455] 225 Probanden der Technischen Universität Berlin werden vor die (nicht verpflichtende) Aufgabe gestellt, sich für den Kauf eines Produkts zwischen zwei möglichen fiktiven Online-Händlern zu entscheiden. Die Probanden erhalten eine Vergütung für die Teilnahme plus zusätzlich eine Subvention beim Kauf eines Produkts. Während beide Händler zum Kaufabschluss transaktionsabhängige Daten (Name, Anschrift, E-Mail-Adresse) benötigen, sind bei Händler 1 mehr sensitive Daten (Geburtsdatum und monatliches Einkommen), bei Händler 2 weniger sensitive Daten (Geburtsjahr, Lieblingsfarbe) verpflichtende Angaben. Alle Produkte werden bei Händler 1 lediglich 1 Euro günstiger angeboten als bei Händler 2. Somit wurden die Probanden mit dem Trade-Off konfrontiert, sensible Daten zu schützen oder aber einen (geringen) Preisdiskont für deren Preisgabe zu erhalten. Im Ergebnis entschieden sich 39 von 42 Käufern für den günstigeren Händler, der zum Abschluss der Transaktion sensiblere Daten einfordert.

Diese Studie verdeutlicht eindrucksvoll, dass der Privatheit in konkreten Entscheidungssituationen ein sehr geringer Stellenwert zugeordnet wird, wenn der Preisgabe der Information ein (wenn auch noch so geringer) Nutzen gegenübersteht. Eine mögliche Erklärung für dieses Verhalten ist, dass mit dem Nutzen der Preisgabe der Daten im Jetzt eine Delegation der (möglichen) Kosten in die Zukunft einhergeht. Acquisti und Grossklags bezeichnen diese Handlungsgrundlage als hyperbolische Diskontierung: Die mit einem exponentiell ansteigenden Diskontierungssatz gewichteten, zukünftig möglichen Kosten unterliegen dem Vorteil der Nutzung im Jetzt.[456] Verdeutlicht an einem Beispiel: Der Nutzen einer Zigarette im Jetzt spielt für den Raucher eine viel stärkere Rolle als der nicht notwendigerweise auf den Konsum zurückzuführende zukünftige Tod. Das Individuum optimiert nach dieser Studie kurzfristig und ein-dimensionierend.

453 Acquisti 2009.
454 Acquisti / Grossklags 2007.
455 Beresford / Kübler / Preibusch 2010.
456 Acquisti / Grossklags 2003.

Das bereits angeführte Experiment von Berendt, Günther und Spiekermann zur Klassifikation der Endverbraucher untersucht nun in einem zweiten Schritt das Verhalten dieser Kurzoptimierer in tatsächlichen Entscheidungssituationen.[457] Die Probanden werden in zwei Gruppen unterteilt und vor die Aufgabe gestellt, in einem Online-Shop ein Produkt zu kaufen: Gruppe 1 erhält bei der Anmeldung im entsprechenden Online-Shop einen Verweis darauf, dass die erhobenen Daten einer dritten Partei zukommen werden, die Daten allerdings gemäß des europäischen Datenschutzrechtes (95/46/EC) behandelt werden. Gruppe 2 erhält lediglich einen Verweis auf die Weitergabe der Daten und der nicht-bekannten Weiterverwendung durch den Datenempfänger. Um das möglichst bestpassende Produkt auszuwählen, werden beide Gruppen von einem „Shopping Bot" unterstützt, der gezielt nach produktspezifischen Anforderungen Fragen stellt. Zusätzlich werden allerdings auch nicht-produktspezifische Fragen gestellt, die einerseits die Produktempfehlung beeinflussen (persönliche Informationen über Vorlieben oder Gewohnheiten im Umgang mit entsprechender Produktkategorie) und andererseits gänzlich vom Produkt losgelöste Fragen (beispielsweise persönliche Einstellung gegenüber Trendentwicklung).

Als Ergebnis zeigt sich einerseits, dass die Granularität der persönlichen Angaben in Gruppe 1 die von Gruppe 2 übersteigt: Hierdurch wird vor allem der Stellenwert von Vertrauen sichtbar: Je größer das Vertrauen in den potenziellen Transaktionspartner ist, desto bereitwilliger werden Informationen preisgegeben. Als zweiter wichtiger Fakt lässt sich eine in erheblichem Maße stattfindende Abweichung von den vorher angegebenen Privatheitsansprüchen der Probanden erkennen: 78 Prozent der Nutzer, die in der vorherigen Befragung der Wahrung ihrer Privatsphäre einen äußerst hohen Stellenwert zugesprochen haben, geben in der konkreten Situation neben produktspezifischen Präferenzen auch persönliche Informationen preis, die mit dem eigentlichen Produkt nicht in Verbindung stehen. Es wird demnach die These gestärkt, dass die ursprünglich formulierte Wertung der Privatheit in dem Moment verworfen wird, wo ihrer Aufgabe ein direkter Nutzen sowie nicht direkt wirksam werdende (und somit hyperbolisch diskontierte) Kosten gegenüberstehen.

Sayre und Horne untersuchen das Nutzerverhalten mit Rabattkarten.[458] Hierfür führen die Autoren in einem ersten Schritt Tiefeninterviews mit einer willkürlichen Auswahl von zwölf Probanden zwischen 23-79 Jahren durch, die eine Rabattkarte besitzen und diese auch verwenden. Das Ziel der Befragung bestand einerseits darin festzustellen, ob sich die Probanden der Verwendung der gesammelten Daten durch den Kartenbetreiber bewusst sind und ob sie andererseits durch die Gewährung von Leistungen bereitwillig darüber hinwegsehen und Daten wie beispielweise ihre Kaufhistorie und Präferenzen preisgeben. Im Ergebnis zeigen lediglich zwei der Probanden ein Unverständnis über die Nutzung der gesammelten Daten seitens der Kartenbetreiber. Die restlichen Probanden zeigen einerseits Verständnis für mögliche Folgen der Datenpreisgabe, auf der anderen Seite allerdings auch eine gewisse Gleichgültigkeit diesbezüglich.

Im zweiten Teil der Studie führen die Autoren eine einmonatige, stichprobenartige Beobachtung innerhalb eines mit Rabattkarten arbeitenden Shops durch. Zusätzlich werden kurze Interviews mit 114 Kunden geführt und ein Fragebogen an 200 Kunden ausgehändigt. Als Ergebnis zeigt sich einerseits, dass mehr als 72 Prozent der Beobachteten eine Rabattkarte besitzen und gar 20 Prozent dieser ihr Kaufverhalten gezielt an Rabattkartenangeboten ausrichten. Durch diese Studie wird verdeutlicht, dass das Privacy Paradox ein nicht nur in der Internetdomäne auftretendes Phänomen darstellt, sondern immer dann beobachtet werden kann, wenn ein möglicher Tausch von Privatheit gegen Leistung möglich wird.

457 Berendt / Günther / Spiekermann 2005.
458 Sayre / Horne 2000.

Wo im stationären Handel meist monetäre Vergünstigungen in Form von Rabatten oder Ähnlichem den Kunden dazu verlocken, Teile seiner Privatheit aufzugeben, wird im Web 2.0 mittels der Bereitstellung (scheinbar) freier Dienste wie Suchmaschinen, sozialen Netzwerken oder Ähnlichem die Datenakquise seitens der Unternehmen vorangetrieben. Diese datenzentrierten Dienste des Web 2.0 erfreuen sich derzeit größter Beliebtheit. Dies zeigt nicht zuletzt die Aufnahme des Verbes „googeln" in den Rechtschreibeduden im Jahr 2004. Auch die Anzahl aktiver Facebook-Nutzer in Deutschland wächst stetig weiter. Aktuell verzeichnet Facebook mehr als 23 Millionen aktive Nutzer in Deutschland.[459] Auch der *Fall Sony* bestätigt dieses Verhalten. Trotz des massiven Diebstahls sensibler Daten von ca. 77 Millionen betroffener Nutzer, den Sony im April 2011 offenbarte, läuft der Playstation-Network-Dienst wieder unter normalen Bedingungen und erfreut sich gar einer gesteigerten Beliebtheit.[460] Das stetig wachsende Interesse steht in direktem Kontrast zu dem oben empirisch belegten Bewusstsein der Endverbraucher über möglicherweise entstehende Privatheitsrisiken. Beispielhaft können Stalking, Identitätsdiebstahl und -betrug, Preisdiskriminierung oder Erpressung das Resultat der Nutzung eines auf den ersten Blick freien Dienstes sein, die in Form von Kosten für den Konsumenten erst nach der eigentlichen Nutzung des Dienstes schlagend werden können.[461] Zudem ist es ein offenes Geheimnis, dass die Wirtschaft sich Facebook oder andere Portale wie LinkedIn zunutze macht, um zum Beispiel Persönliches über Bewerber zu erfahren.

Acquisti und Gross untersuchten das Offenbarungsverhalten von College-Studenten bei der Nutzung von Facebook.[462] Die Teilnehmer wurden ohne das Wissen über den Inhalt der Studie rekrutiert. Von den 318 teilnehmenden Probanden zeigten lediglich 40 kein Interesse an der Nutzung von Facebook. Von den übrigen 278 Probanden bekundete die überwältigende Mehrheit eine aktive Nutzung (70,8 Prozent) während lediglich 2,5 Prozent über einen inaktiven Account und 26,7 Prozent über keinen Account verfügten. Die Interesse bekundenden Probanden wurden nun mittels eines Fragebogens in einem ersten Teil über das nicht-Facebook-spezifische Privatheitsempfinden, in einem zweiten Schritt über Facebook-spezifisches Wissen und Verhalten interviewt. Als ein erstes (zu erwartendes) Resultat zeigt sich, dass die Probanden, die Facebook nicht nutzen, ein höheres Privatheitsempfinden aufweisen als Facebook-Nutzer. Die statistische Auswertung zeigt allerdings weiterhin, dass von einem höheren Privatheitsempfinden nicht direkt auf eine geringere Nutzungshäufigkeit geschlossen werden kann. Diese Feststellung ist eine Bestätigung des Privacy Paradoxons. Dem Wissen über mögliche Privatheitskonsequenzen steht der Wille entgegen, den Dienst trotz bestehender Gefahren zu nutzen.

Um nun herauszufinden, worin die Gründe dafür liegen, Facebook trotz vorher geäußerter Privatheitssorgen zu nutzen, untersuchen die Autoren die Motivation zur Nutzung des Dienstes. Als Resultat zeigt sich, dass die stärkste Triebkraft zur Nutzung dieses Dienstes in der Pflege von bereits bestehenden Kontakten beziehungsweise Freundschaften durch bessere Kontaktmöglichkeit sowie bessere Informationsgewinnung liegt. Andere Gründe, wie beispielweise das Auffinden von Gleichgesinnten oder aber die Vergrößerung des Freundeskreises, werden weniger stark gewichtet. Somit kann festgestellt werden, dass möglichen Privatheitsrisiken, die eine Nutzung mit sich bringt, ein gesellschaftlicher Schaden bei Verweigerung, wie etwa ein Entfernen oder weiterführend gar ein Ausschluss vom Freundeskreis, gegenübersteht. Diese Feststellung spricht für die These, dass ein Individuum primär gesellschaftliche Integration und Anerkennung wünscht. Erst sekundär werden Gefahren gewertet. Es gibt somit rational keine Möglichkeit des Opt-Outs. Dies ist ein Fakt, der bei bisherigen Untersuchungen des Privacy Paradox nicht berücksichtigt wurde.

459 Statista 2012.
460 HDDaily 2011.
461 Acquisti 2011.
462 Acquisti / Gross 2006.

Chapin, Santell und Greenstadt untersuchten die Wahrnehmung und Auswirkung von Privatheitsvorfällen anhand öffentlich gewordener Vorfälle von Apple (Aufzeichnung von Ortungsdaten der iOS-Software), Facebook (Änderung der Privatheitsregelung) und Sony (Diebstahl von Nutzerdaten des Playstation Networks) anhand eines Probandenexperimentes mit 200 Teilnehmern.[463] Ein Kriterium zur Teilnehmerauswahl bestand darin, dass diese bereits vor Bekanntmachung des Vorfalls ein iOS Gerät, PSN- oder Facebook-Account besitzen mussten und weiterhin verwenden, um somit die Auswirkungen auf die tatsächlich bestehende Nutzung sowie die Wahrnehmung der anderen Dienste nach der Veröffentlichung zu untersuchen. Der nun von den Probanden zu beantwortende Bogen enthält Fragen bzgl. der Tendenz zur zukünftigen (Weiter-)Nutzung der drei Dienste. Die Antwortmöglichkeiten beinhalten (1) die totale Verweigerung, (2) eine sinkende Tendenz, (3) eine nicht veränderte sowie (4) eine steigende Tendenz, den Dienst aufgrund des Vorfalls künftig zu nutzen. Als Resultat zeigt sich, dass die Mehrheit der Facebook-Nutzer (56 Prozent) keinerlei Tendenz zeigen, die Verwendung des Dienstes aufgrund des Privatheitsvorfalls zu ändern. 42 Prozent der Sony-PSN-Mitglieder gaben an, ihre Nutzung künftig nicht zu verändern, während 31 Prozent eine sinkende Tendenz voraussagten. Eine gleichbleibende Nutzungstendenz zeigen 35 Prozent der iOS-Nutzer, während 36 Prozent eine sinkende Nutzungstendenz aufgrund des Privatheitsvorfalls angeben.

Die Ergebnisse zeigen, dass die Billigung von möglichen Privatheitsrisiken je nach verwendetem Dienst unterschiedliche Ausprägungen aufweisen. Dies lässt sich auf die spezifisch entstehenden Kosten auch nur kurzfristiger Verweigerung zurückführen. Während die Nutzung beziehungsweise deren Verweigerung eines iOS-Gerätes beispielweise keinerlei gesellschaftliche Implikationen nach sich zieht, kann die Verweigerung der Nutzung eines sozialen Netzwerkes, beispielweise Facebook, wie oben angeführt starke gesellschaftliche Nachteile oder sogar zu Ausschluss führen. Somit können aus der Verweigerung, einen Dienst zu nutzen, Konsequenzen resultieren. Hieraus lässt sich ableiten, dass der Erfolg eines datenzentrierten Geschäftsmodelles im Web 2.0 darauf beruht, die Kostenlosigkeit des Dienstes zu dessen Manifestierung im gesellschaftlichen Alltag zu nutzen, dessen Absenz als nicht mehr denkbar erscheint und dass daher ein „Opt-Out" nicht möglich ist.

3.7 HERAUSFORDERUNG AN PRIVATHEITSMECHANISMEN

Internet Privacy unterscheidet sich von der sonstigen Privatsphäre nur dadurch, dass informatische Mechanismen angewendet werden müssen, um persönliche Daten zu schützen. Solche Mechanismen basieren auf den Prinzipien der Zugangskontrolle, die letztlich aus den Phasen Identifikation und Erlaubnis oder Ablehnung besteht. Eine Betrachtung von Eigenschaften der gegenwärtigen Privatheitsmechanismen und den wirtschaftlichen Anforderungen ergibt erweiterte und ergänzende Anforderungen. Danach liegt der Akzeptanzmangel gegenwärtiger PET-Technologie an ihren Voraussetzungen oder an ihrem für wirtschaftliche Notwendigkeiten unzureichendem Technikmodell. PET realisieren das Verbergen und die Zugangskontrolle zu persönlichen Daten, während alle wirtschaftlichen Nutzungen sich auf die Verwendung der Daten konzentrieren. PET bieten aber keinerlei Unterstützung für die Kontrolle der Datennutzung. Am Beispiel der Entwicklung von P3P (*The Platform for Privacy Preferences*) zum Schutz von Web-Sites zeigt sich, dass dieser Mangel zu einer Verweigerung der Technologie durch Nutzer führt. So kontrolliert P3P heute wirkungsvoll die Cookies, aber nicht ihren eigentlichen Zweck. Dies gilt in ähnlicher Form für alle anderen PET-Mechanismen,[464] die die Realisierung von Transparenz vermissen lassen. Dashboards, wie unter anderem Google sie anbietet, sind solche Screening- und

[463] Chapin / Santell / Greenstadt 2011.
[464] Federrath 2005.

Signalling-Technologien. Die Nachteile sind offensichtlich, da noch keine Garantien vorliegen, dass die gesamten aggregierten Daten vom Anbieter offengelegt werden. Eine Vertrauensinfrastruktur müsste dieses fehlende Vertrauen schaffen. Eine weitere Begründung für die Defizite der PET-Mechanismen liegt darin, dass PET auf den Schutz persönlicher Daten ausgerichtet sind, während für die wirtschaftliche Verwertbarkeit eine statistische Genauigkeit genügt. Die nachfolgenden vier Fragen zu den PET-Technologien verdeutlichen deren aktuelle Defizite und geben Hinweise auf ein neues Privatheit unterstützendes Technikmodell für datenzentrische Dienste:[465]

1. Die größte Gefahr für die Privatheit kommt von einem unautorisierten Zugang zu Informationen?

Die Kryptologie als die Königsdisziplin der Sicherheit hält Informationen vor Unberechtigten geheim. Nur dazu müssen sich die Kommunizierenden vertrauen, während sie sich bei Privatheit eben nicht vertrauen. Werkzeuge der sogenannten PET-Technologie versetzen den Nutzer theoretisch in die Lage, Wünsche zu formulieren und auch durchzusetzen. Die Annahme ist, dass er dies kann und auch will. Das Kalkül der Nutzer lautet jedoch meist anders. Sie setzen eher auf Anreize und weniger auf Gefahren. Privatheitsverlust ist eine Gefahr, die Realisierung zum Beispiel von Konsumentenrenten ein Gewinn. Diese Beobachtung verleitet gerne zu dem Schluss, dass die Privatheit dem Einzelnen nicht viel wert ist.

2. Privatheit ist dann gegeben, wenn keine Personen-identifizierende Informationen (PII) erfasst sind?

Wäre dies der Fall, hätte kein Dienst des Web 2.0 und auch kein Sammeldienst Probleme mit der Privatheit. Wirtschaftlich sind wirklich persönliche Daten nicht weiter interessant. Es geht nicht so sehr um den Einzelnen, sondern um eine korrekte statistische Klassifikation, meist in Bezug auf deren Zahlungsbereitschaft und Bonität.

3. Schulungen und Optionen zur Wahl der Formen und des Ausmaßes der Privatheit sind die Grundpfeiler der informationellen Selbstbestimmung?

Häufig wird der Wunsch nach Privatheit mit dem Argument verneint, dass man ja nichts Peinliches zu verbergen hat und deshalb auch kein Problem habe sollte, wenn Daten über einen gesammelt werden. Dies führt zu einer sorgenfreien Negierung der Warnungen der Dienstanbieter. Schulungen allgemeiner Art sowie seitenlange allgemeine Nutzervereinbarungen werden wie auch andere Schulungen ignoriert.

4. Datenschutz ist eine Sache über Individuen?

In zahlreichen Fällen sammeln datenzentrische Dienste keine Daten über Individuen. Es geht nicht um die Ausprägung persönlicher Daten, sondern um deren Verwendung.

LITERATUR

Accorsi 2008a
Accorsi, R.: *Automated Counterexample-Driven Audits of Authentic System Records*. Dissertation, Universität Freiburg 2008.

Accorsi 2008b
Accorsi, R.: *Automated privacy audits to complement the notion of control for identity management*. IFIP Conference on Policies and Research in Identity Management. Springer 2008.

Accorsi / Sato / Kai 2008
Accorsi, R. / Sato, Y. / Kai, S.: „Compliance-Monitor zur Frühwarnung vor Risiken". In: *Wirtschaftsinformatik* 50(5) (2008), S. 375-382.

[465] Müller 2011.

Ackermann / Cranor / Reagle 1999
Ackerman, M. / Cranor, L. / Reagle, J.: *Privacy in e-commerce: examining user scenarios and privacy preferences*. Proceedings of the 1st ACM conference on Electronic commerce 1999

Acquisti 2009
Acquisti, A.: „Nudging Privacy The Behavioral Economics of Personal Information". In: *IEEE Security & Privacy* Vol 7 No. 6, 2009, S. 72-75.

Acquisti 2011
Acquisti, A.: *SPION. Agentschap voor Innovatie door Wetenschap en Technologie* 2011.

Acquisti / Gross 2006
Acquisti, A. / Gross, R.: *Imagined communities: Awareness, information sharing and privacy on the Facebook*. PET 2006.

Acquisti / Grossklags 2003
Acquisti, A. / Grossklags, J.: *Losses, gains and hyperbolic discounting: An experimental approach to information security attitudes and behaviour*. 2nd Annual Workshop on Economics and Information Security 2003.

Acquisti / Grossklags 2007
Grossklags, J. / Acquisti, A.: *When 25 Cent is too much: An experiment on willingness-to-sell and willingness-to-protect personal information*. Proceedings og the 6th Workshop on the Economics of Information Security (WEIS) 2007.

Adomavicius / Tuzhilin 2005
Adomavicius, G. / Tuzhilin, A.: „Personalization technologies: a process-oriented perspective". In: *Communications of the ACM*, 48 (10) 2005.

Anderson 2010
Anderson, C.: *Free: How today's smartest businesses profit by giving something for nothing*. Random House UK 2010.

Apel / Behme / Eberlein / Merighi 2009
Apel, D. / Behme, W. / Eberlein, R. / Merighi, C.: *Datenqualität erfolgreich steuern - Praxislösungen für Business-Intelligence-Projekte*, Carl Hanser und TDWI 2009.

Armbrust 2009
Armbrust et al.: *Above the Clouds - A Berkeley View of Cloud Computing*, Technical Report No. UCB/EECS-2009-28, February 10, 2009, URL: http://www.eecs.berkeley.edu/Pubs/TechRpts/2009/EECS-2009-28.pdf.

Bapna / Jank / Shmueli 2008
Bapna, R. / Jank, W. /Shmueli, G.: „Consumer Surplus in Online Auctions". In: *Information Systems Research* 19(4) 2008. URL: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=840264.

Benisch / Kelley / Sadeh / Cranor 2011
Benisch, M. / Kelley, P. G. / Sadeh, N. M. / Cranor, L. F.: „Capturing location-privacy preferences: quantifying accuracy and user-burden tradeoffs". In: *Personal and Ubiquitous Computing* 15(7) 2011, 679-694.

Berendt / Günther / Spiekermann 2005
Berendt, B. / Günther, O. / Spiekermann, S.: „Privacy in E-Commerce: Stated Preferences vs. Actual Behaviour". In: *Communications of the ACM* Vol. 48 No. 4 (2005) S. 101-106.

Beresford / Kübler / Preibusch 2010
Beresford, A. / Kübler, D. / Preibusch, S.: *Unwillingness to Pay for Privacy: A Field Experiment*. IZA Discussion Paper No. 5017 (2010).

BITKOM 2011
BITKOM: *Soziale Netzwerke - Eine repräsentative Untersuchung zur Nutzung sozialer Netzwerke im Internet*. 2011.

Böhme 2008
Böhme, R.: *Conformity or Diversity: Social Implications of Transparency in Personal Data Processing*. 2008.

Boyd 2010
Boyd, d.: *Privacy and Publicity in the Context of Big Data*. WWW 2010 conference, 2010.

Brynjolfsson / Smith / Hu 2003
Brynjolfsson, E. / Smith, M. / Hu, Y.: *Consumer surplus in the digital economy: Estimating the value of increased product variety at online booksellers*, Management Science 2003.

Brynjolfsson / Saunders 2010
Brynjolfsson, E. / Saunders, A.: *Wired for Innovation*, MIT Press 2010.

Brynjolfsson / Hitt / Kim 2011
Brynjolfsson, E. / Hitt, L. / Kim, H.: *Strength in Numbers: How Does Data-Driven Decisionmaking Affect Firm Performance?* (April 22, 2011). Available at SSRN: URL: http://ssrn.com/abstract=1819486.

Campbell / Gordon / Loeb / Zhou 2003
Campbell, K. / Gordon, L. / Loeb, M. / Zhou, L.: „The Economic Cost of Publicly Announced Information Security Breaches: Empirical Evidence from the Stock Market". In: *Journal of Computer Security*, 11 (2003) 3, S. 431–448

CDT 2009
Center for Democracy and Technology: Survey Information: Americans Care Deeply About Their Privacy (October 22, 2009). URL: https://www.cdt.org/privacy/guide/surveyinfo.php

Chapin / Santell / Greenstadt 2011
Chapin, A. / Greenstadt R. / Santell, J.: *How Privacy Flaws Affect Consumer Perception, unpublished manuscript*. 2011.

Chamoni / Gluchowski 1997
Chamoni, P. / Gluchowski, P.: *Analytische Informationssysteme, Business Intelligence-Technologien und -Anwendungen*. Springer 1997.

Chaum 1981
Chaum, D.: *Untraceable electronic mail, return addresses, and digital pseudonyms*, Communications of the ACM. 1981.

Chow 2009
Chow, R.: *Controlling Data in the Cloud*, CSCW 09, 2009.

Cooley / Mobasher / Srivastava 1997
Cooley, R. / Mobasher, B. / Srivastava, J.: *Web mining: information and pattern discovery on the World Wide Web*, Proc. of the Ninth IEEE International Conference on Tools with Artificial Intelligence 1997.

Culnan / Armnstrong 1999
Culnan, M. / Armnstrong, P.: „Information Privacy Concerns, Procedural Fairness, and Impersonal Trust: An Empirical Investigation". In: *Organization Science* Vol. 10 No. 10 (1999), S. 104-115.

Davenport 2009
Davenport, T.: H*ow to Design Smart Business Experiments*, Harvard Business Review, 2009.

FAZ 2011a
FAZ: „Facebook hat erst 1 Prozent seines Weges geschafft". In: Wirtschaftsteil der *Tageszeitung* vom 27.11.2011.

FAZ 2011b
FAZ: „Online-Werbung legt jedes Jahr mehr als 10 % zu", In: Wirtschaftsteil der *Tageszeitung* vom 27.11.2011.

Federrath 2005
Federrath, H.: „Privacy Enhanced Technologies: Methods – Markets – Misuse". In: Kalsikas, S et. al., *Trustbus* 2005, LNCS 3592, 2005, S. 6-11.

Flender / Müller 2012
Flender, C. / Müller, G.: „Type Indeterminacy in Privacy Decisions: The Privacy Paradox Revisited", to appear in: *Proceedings of the 6th International Symposium on Quantum Interaction* (QI 2012), Paris School of Economics, Springer 2012.

FoA 2011
FoA: „Studie Future of Advertising 2015", In: Arthur D. Little, *denkwerk*, eco, IP Deutschland, memi, Medien.NRW, September 2011.

Gartner 2011a
Gartner, Inc.: Gartner Executive Programs Worldwide Survey of More Than 2,000 CIOs Identifies Cloud Computing as Top Technology Priority for CIOs in 2011. URL: http://www.gartner.com/it/page.jsp?id=1526414

Gartner 2011b
Gartner, Inc.: Gartner Says Solving ‚Big Data' Challenge Involves More Than Just Managing Volumes of Data (June 27, 2011). URL: http://www.gartner.com/it/page.jsp?id=1731916

Ghose 2009
Ghose, A.: *Internet Exchanges for Used Goods: An Empirical Analysis of Trade Patterns and Adverse Selection*, MIS Quarterly, 2009.

Ghose / Smith / Telang 2006
Ghose, A. / Smith, M. /Telang, R.: *Internet Exchanges for Used Books: An Empirical Analysis of Product Cannibalization and Welfare Impact, Information Systems Research*, 2006.

Goolsbee / Petrin 2004
Goolsbee, A. / Petrin, A.: *The consumer gains from direct broadcast satellites and the competition with cable TV*, Econometrica 2004.

Harris 1994
Harris, L.: *Harris-Equifax Consumer Privacy Surveys*, 1990-1994. Atlanta, GA: Equifax, Inc., 1994.

HDDaily 2011
HDDaily: Sony: PSN-Hack hat viele inaktive Nutzer zurückgebracht, 2011. URL: http://www.hddaily.de/2011/10/25/sony-psn-hack-hat-viele-inaktive-nutzer-zuruckgebracht-33637.html

Hinz / Eckert 2010
Hinz, O. / Eckert, J.: „Der Einfluss von Such- und Empfehlungssystemen auf den Absatz im Electronic Commerce". In: *WIRTSCHAFTSINFORMATIK*, 52 (2), 2010, S. 65-77.

Hitachi 2011
Hitachi: *E-Identity Report, Interner Forschungsbericht des Instituts für Informatik und Gesellschaft (IIG)*, Universität Freiburg 2011.

IWF 2011
Institut der deutschen Wirtschaft (IWF): *Faktor Google: Wie Deutsche Unternehmen Google einsetzen*, Köln, 2011.

Kaiser 2003
Kaiser, J.: „Besteht eine Beziehung zwischen Nutzbarkeit und Sicherheit?" In: *Praxis der Informationsverarbeitung und Kommunikation* Vol. 26 No. 1 (2003), S. 48-51.

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

Kolo / Meyer-Lucht 2007
Kolo, C. / Meyer-Lucht, R.: „Erosion der Intensivleserschaft. Eine Zeitreihenanalyse zum Konkurrenzverhältnis von Tageszeitungen und Nachrichtensites". In: *Medien & Kommunikationswissenschaft* 8(4), 2007, S. 513-533.

Kumaraguru / Cranor 2005
Kumaraguru, P. / Cranor, L.: *Privacy Indexes: A Survey of Westin's Studies*. ISRI Technical Report, 2005.

Müller 2008
Müller, G.: „Information Security: 50 years behind, 50 years beyond." In: *Wirtschaftsinformatik* 50(4), 2008, Für Sie gelesen, S. 322-323.

Müller 2010a
Müller, G.: *Weiß Google mehr als ein „Geheimdienst"?* Special Workshop LAW, 7. Internationales Meschenrechtsforum Luzern (IHRF), 18./19. Mai, 2010.

Müller 2010b
Müller, G.: „Datenschutz: Ein Auslaufmodell?". In: *Digma*, März 2010, S. 85 ff.

Müller 2011
Müller, G.: *Die Mythen von Transparenz und Sicherheit im Internet, Ansprache zur Verleihung der Ehrendoktorwürde der TU Darmstadt*. URL: http://www.telematik.uni-freiburg.de/system/files/Ansprache.pdf. 2011.

Müller / Eymann / Kreutzer 2003
Müller, G. / Eymann, T. / Kreutzer, M.: *Telematik- und Kommunikationssysteme in der vernetzten Wirtschaft*, S. 302 – 304, Lehrbücher Wirtschaftsinformatik, Oldenbourg 2003.

Müller / Rannenberg 1999
Müller, G. / Rannenberg, K.: „Multilateral Security. Empowering Users, Enabling Applications". In: Müller, G. et al. (Hrsg.): *Multilateral Security in Communications. Technology, Infrastructure, Economy*, S. 563-570, Addison-Wesley-Longman 1999.

Müller / Sonehara / Echizen / Wohlgemuth 2011
Müller, G. / Sonehara, N. / Echizen, I. / Wohlgemuth, S.: „Nachhaltiges Computing in Clouds". In: Wirtschaftsinformatik S3(3), 2011, S. 123-125

Poscher 2012
Poscher, R.: „Die Zukunft der informationellen Selbstbestimmung als Recht auf Abwehr von Grundrechtsgefährdungen". In: Gander et al. (Hrsg.): *Resilienz in der offenen Gesellschaft*, Nomos Verlag 2012.

Pretschner / Hilty / Schaefer et al. 2008
Pretschner, A. / Hilty, M. / Schaefer, C. et al.: Usage Control Enforcement: Present and Future. IEEE Security and Privacy, Vol. 6(4), 2008, S. 44-53.

Prüser 2011
Prüser, S.: *Die Cloud in aller Munde - aber noch längst nicht im Handel*, Heise resale, Hannover, 2011

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

Sackmann / Strüker / Accorsi 2006
Sackmann, S. / Strüker, J. / Accorsi, R.: „Personalization in Privacy-Aware in Highly Dynamic Systems". In: *Communications of the ACM*, 49(9), 2006.

Sayre / Horne 2000
Sayre, S. / Horne, D.: „Trading Secrets for Savings: How concerned are Consumers about Club Cards as a Privacy Threat?" Advances In: *Consumer Research* Vol 27, 2000, S. 151-155.

Shapiro / Varian 1999
Shapiro, C. / Varian, H.: *Information rules: a strategic guide to the network economy*. Harvard Business School Press: Boston, Mass., 1999.

Slobogin 2012
Slobogin, C.: „Regulation of Government Surveillance under the United States Constitution". In: Gander et al. (Hrsg.): *Resilienz in der offenen Gesellschaft*, Nomos Verlag 2012.

Smith / Milberg / Burke 1996
Smith, H. / Milberg, S. / Burke, S.: „Information Privacy: Measuring Individualss' Concerns about Organizational Practices". In: *MIS Quarterly* Vol. 20 No. 2, 1996, S. 167-196.

Statista 2011
Statista: Umsätze der Onlinewerbung in Deutschland von 2005 bis 2015 (in Millionen Euro), 2011. URL: http://de.statista.com/statistik/daten/studie/165473/umfrage/umsatzentwicklung-von-onlinewerbung-seit-2005/

Statista 2012
Statista: Anzahl der aktiven Nutzer von Facebook in Deutschland von Juli 2009 bis Juli 2012 (in 1.000), 2012. URL: http://de.statista.com/statistik/daten/studie/70189/umfrage/nutzer-von-facebook-in-deutschland-seit-2009/

Statistisches Bundesamt 2010
Statistisches Bundesamt: *Statistisches Jahrbuch 2010 für die Bundesrepublik Deutschland*, S. 260 https://www.destatis.de/DE/Publikationen/StatistischesJahrbuch/StatistischesJahrbuch2010.pdf?__blob=publicationFile. 2010.

Strüker / Sackmann / Müller 2004
Strüker, J. / Sackmann, S. / Müller, G.: *Case study on retail customer communication applying ubiquitous computing*, Proc. of Int. Conference on e-Commerce Technology, IEEE, 2004, p. 42-48.

SVR-Gesundheit 2009
SVR-Gesundheit: *Gutachten des Sachverständigenrates zur Begutachtung der Entwicklung im Gesundheitswesen*, 2009, S. 36.

Varian 1996
Varian, H.: *Economic Aspects of Personal Privacy*, 1996.

Varian 2011
Varian, H.: *Grundzüge der Mikroökonomik*, Oldenbourg, 8. Auflage, 2011.

Webster 2011
Webster, J.,: *Big Data: How New Analytic Systems will Impact Storage*, SNW 2011.

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

Wohlgemuth 2009
Wohlgemuth, S.: *Privatsphäre durch die Delegation von Rechten*, Dissertation Institut für Informatik und Gesellschaft (IIG), Universität Freiburg, Vieweg + Teubner, Wiesbaden 2009.

Whitten / Tygar 1999
Whitten, A. / Tygar, J.: „Why Johnny Can`t Encrypt: A Usability Evaluation of PGP 5.0." In: *Proceedings of the 8th USENIX Secutity Symposium*, 1999.

Yao 1982
Yao, A.: *Protocols for Secure Computations*, IEEE, 1982.

4 STATE OF ONLINE PRIVACY: A TECHNICAL PERSPECTIVE

FLORIAN KELBERT, FATEMEH SHIRAZI, HERVAIS SIMO, TOBIAS WÜCHNER, JOHANNES BUCHMANN, ALEXANDER PRETSCHNER, MICHAEL WAIDNER

ABSTRACT

Recent years have seen an unprecedented growth of Internet-based applications and offerings that have a huge impact on individuals' daily lives and organisations' (businesses and governments) practices. These applications are bound to bring large-scale data collection, long-term storage, and systematic sharing of data across various data controllers i.e., individuals, partner organizations, and scientists. This creates new privacy issues. For instance, emerging Internet-based applications and the underlying technologies provide new ways to track and profile individual users across multiple Internet domains, often without their knowledge or consent. In this section, we present the current state of privacy on the Internet. The section proposes a review and analysis of current threats to individual privacy on the Internet as well as existing countermeasures. Our analysis considers five emerging Internet-based applications, namely personalized web and E-commerce services, online social networks, cloud computing applications, cyber-physical systems, and Big data. It outlines privacy-threatening techniques, with a focus on those applications. We conclude with a discussion on technologies that could help address different types of privacy threats and thus support privacy on the Web.

ZUSAMMENFASSUNG

Internetbasierte Anwendungen und Angebote haben in den vergangenen Jahren enorme Verbreitung gefunden und prägen heutzutage sowohl die Lebensgestaltung Einzelner als auch Vorgänge in Unternehmen und öffentlichen Einrichtungen. Diese Anwendungen gehen einher mit umfassender Datensammlung, langjähriger Datenspeicherung sowie gezielter Datenweitergabe zwischen Einzelpersonen, Partnerunternehmen und Wissenschaftlern. Hierdurch entstehen noch nie dagewesene Datenschutzprobleme. Beispielsweise ermöglichen internetbasierte Anwendungen und die hierin genutzten Technologien die Profilbildung und Verfolgung einzelner Nutzer über mehrere Internetzonen hinweg – oftmals ohne Wissen oder Einverständnis der Nutzer. In diesem Abschnitt gehen wir auf den aktuellen Stand der Technik im Hinblick auf Privatsphäre und Datenschutz im Internet ein. Hierzu werden die gegenwärtigen Bedrohungen im Hinblick auf Privatsphäre sowie existierende Gegenmaßnahmen beschrieben und analysiert. Die Analyse basiert auf fünf neuartigen internetbasierten Anwendungen: personalisierte Web- und E-Commerce-Angebote, soziale Online-Netzwerke, Cloud Computing, Cyber-Physical Systems und Big Data. Nach Beschreibung dieser Anwendungen werden zunächst die Privatsphäre-bedrohenden Techniken, die verstärkt im Internet eingesetzt werden, erläutert. Anschließend werden Technologien erörtert, die bei entsprechendem Einsatz den Bedrohungen entgegenwirken können und somit Privatsphäre im Internet fördern.

4.1 INTRODUCTION

The Internet has become part of daily life for billions of users worldwide.[466] Individuals are increasingly reliant on the Internet as the primary medium for finding information of all kinds, interacting with peers and public authorities, for representing and managing their online social ties, and for purchasing and/or delivering goods and services online. Organisations, public and private, on the other hand, are heavily dependent on the Internet when interacting with individuals (customers, citizens, or employees) and for offering personalized online experiences and services. In order to do so, both individuals and organisations typically have to share a huge amount of personal information. The possible privacy and security risks of such practices have been underestimated for many years. According to a number of recent surveys,[467,468,469] a growing number of Internet users have privacy, security, and trust concerns, e.g. when disclosing personal information or purchasing goods online. Indeed, most Internet users left some digital traces such as the IP addresses of their devices, the web pages they visited, the terms they searched for, and their locations. Although users may expect that many of their online activities are anonymous or remain to some extent under their control, both the practices and new business models on the internet allows a myriad of players to collect, compile, and monetize users' information, in some cases without users' knowledge or consent.

The purpose of this chapter is to give a thorough overview of the present state of Internet privacy from the technical perspective. We discuss the privacy threats and risks that individuals are facing when exposed to Internet-based applications, and also investigate the corresponding technical countermeasures and solutions to such privacy threats. We argue that those privacy threats and risks arise due to the ability of various entities (other people, businesses, and government authorities) not only to collect, process, and share large amounts of information about individuals using Internet-based applications, but also the ability of said entities to store that information over a virtually unlimited period of time. We base our analysis on six exemplary real-world applications and scenarios: personalized web and E-commerce services, online social networks, cloud computing applications, cyber-physical systems, and Big data, respectively.

This chapter is organized around three pillars: emerging applications and scenarios, threats, and technical solutions. Section 4.2 examines the opportunities and privacy issues in the context of the chosen Internet applications and scenarios. Following this, Section 4.3 provides a detailed discussion on the techniques and technologies that may cause those privacy risks and threats. Section 4.4 presents existing privacy-enhancing technologies to cope with the introduced privacy threatening techniques. Finally, we provide conclusion in Section 4.5.

4.2 APPLICATIONS AND EMERGING SCENARIOS

The persistent success of the Internet has been accompanied by the emergence of numerous web and mobile applications including web search engines and personalized online commerce.[470,471] To attract and retain customers, and thus increase their revenues and market shares in spite of competition, online service and content providers offer personalized web experiences. Indeed, there is a consistent trend toward adopting web personalization as a strategic business tool. A key characteristic of personalized services

466 http://www.internetworldstats.com/stats.htm
467 Huth/Arns/Budde 2011.
468 Madden 2012.
469 ITU 2011.
470 http://www.pewinternet.org/Trend-Data/Online-Activites-Total.aspx
471 InternetWorldStats 2011.

and applications is that they are customized according to their users' interests and preferences.

Providing a proper definition of the notion of personalization on the web has proven to be a difficult task. Numerous alternative definitions have been published, each covering specific aspects. A simplistic definition by Ho and Tam describes personalization as "[...] delivering the right content to the right person in the right format at the right time".[472] Kobsa et al. describe web personalization in terms of technology being deployed to the Web which takes characteristics of their current users into account and adapts their behaviour accordingly.[473,474] In the specific context of electronic business, the term personalization refers to using personal data to tailor and deliver online services and contents (e.g. personalized news and web search) according to the interests of individual users. This also includes individualizing item recommendations and advertisements based on past purchase and browsing behaviour.[475,476] Personalization is a common approach to attract prospective customers to online services. Indeed, the ever growing popularity of modern web applications is not only due to the fact that they can easily be accessed from almost any location at any time (as long as there is Internet access), but also because they can be tailored according to the interests, preferences and needs of individual users. Some empirical evidence shows that web personalization is increasingly becoming a key marketing instrument for online content/service providers.[477,478,479] Other research results indicate that Internet users, on the other hand, value customizable online experiences.[480,481,482,483]

While the shift towards web personalization is generally viewed favourably by both online service providers and Internet users, it also introduces serious privacy concerns, as the data needed to offer personalized services is often private by its very nature.[484,485] The problem is exacerbated by the advent of digital mobility[486] and modern web offerings such as web search engines and E-commerce features like item recommendation and targeted advertising. These emerging Internet applications and services typically require the collection, aggregation and sharing of information about a user's preferences, browsing and purchase activities, often without their knowledge and control.

4.2.1 WEB SEARCH ENGINES

Search engines like Google, Yahoo!, Baidu and Bing, just to name a few, have today become fundamentally important tools to enhance Internet users' online experience. They provide web search services that tailor search results according to users' preferences. Internet users rely on them when looking for information they might need either for work (e.g. scientific papers) or for leisure, e.g. when planning travel or searching for specific books about, in some instances,

472 Ho/Tam 2005.
473 Kobsa 2003.
474 Kobsa 2001.
475 Eirinaki/Vazirgiannis 2003.
476 Tam/Ho 2005.
477 Chellappa/Sin 2005.
478 Sheng/Nah/Siau 2008.
479 Hagen/Manning/Souza 1999.
480 Goy/Ardissono/Petrone 2007.
481 Ho/Kwok 2003.
482 Tam/Ho 2003.
483 Kobsa 2003.
484 Kobsa 2007.
485 Sackmann/Strüker/Accorsi 2006.
486 PWC 2011.

controversial topics. In order to operate properly, i.e. provide better search results and tailor their services more closely to customer interest, web search engines need to record all visited websites, log information about search queries, and collect other details about interactions with their users, including IP-addresses, HTTP headers, starting times or even session durations. For the same purposes, today's search engines also apply various data mining processes on search query logs and extract fine-grained knowledge about the user.

Web Search Privacy Concerns

Although necessary for achieving customized web search at the individual level, the tracking, aggregation and mining of users' search queries may also provide a new surface for attacks on internet users' privacy.[487,488,489] Indeed, personalization of web search services requires search engines to "accurately" model users' preferences and interests based on knowledge of their past online behaviours. Relying on advanced data mining techniques, and based on the user's search queries and browsing history, search engines can then extract details about the identity, interests, and preferences of that specific individual. Information extracted from the user's search queries may include sensitive details ranging from her intimate emotions, gender and relational status, location history, to her political view, her interest in specific products/content/services, her plans, sexual orientation, hobbies, etc. Much of that information is considered sensitive and very private in nature, but is stored centrally on service providers' servers. In most cases, users have limited access to and control over search logs stored on the providers' side. Exceptions include services like Google history (http://google.com/history).

Usually, Internet users express concerns about services that monitor their (online) activities and accumulate information about them since that data can potentially be misused to perform secondary activities such as spamming, phishing, or unauthorized sharing with third parties (e.g. advertisers).

Besides being used to optimize the quality of the personalized services being delivered, web search logs are viewed by many scientists as unique opportunities to tackle certain challenges which impact modern societies more and more frequently. For instance, biologists might wish to apply statistical methods to web search logs to study the location and time of search queries in an attempt to reconstruct, or even predict, disease outbreaks.[490] Likewise, social scientists would be interested in applying information analytics to search logs when investigating social trends, e.g. unemployment trends in a particular region. However, publishing search logs without effective safeguards poses a real threat to users' privacy. The controversy surrounding the 2006 AOL search data leak illustrates this.[491] When releasing the search queries of approximately 650,000 people, in August 2006, the only significant privacy preserving mechanism AOL decided to deploy was to replace IP addresses with pseudo identities. As a consequence, an investigative reporter was able, based on the released AOL query logs, to identify user No. 4417749 as Ms. Thelma Arnold, a 62-year-old widow from Lilburn, Georgia, USA. Recently, researchers demonstrated that, despite search log robust sanitization processes (i.e. anonymization or obfuscation) being applied, query logs may still contain quasi-identifiers (e.g. user's gender, age, and zip code) which can be used to reversely identify a user or a small set of persons containing that user, with reasonable accuracy.[492,493,494]

487 Castelluccia/Cristofaro/Perito 2010.
488 Turow/King/Hoofnagle/Bleakley/Hennessy 2009.
489 Teltzrow/Kobsa 2004.
490 Ginsberg/Mohebbi/Patel/ Brammer/Smolinski/Brilliant 2009.
491 Barbaro/Zeller 2006.
492 Toubiana/Nissenbaum 2011.
493 Götz/Machanavajjhala/Wang/Xiao/Gehrke 2012.
494 Jones/Kumar/Pang/Tomkins 2007.

Personalized Social Search

As Web 2.0 applications continue to be popular and the amount of social data on the Web is growing rapidly, a new form of personalized online search services is gaining momentum, the personalized social search.[495,496] To optimize and customize search results, emerging social search services leverage social data gathered from Web 2.0 applications, such as wikis, blogs, forums, social bookmarking services, social network sites, and many others.

In contrast to established approaches, social search engines determine the relevance of search results based on recommendations by the searcher's social relations or users with similar preference profiles. In order to capture the searcher's interest profiles, social search applications rely on collaborative filtering methods for the evaluation of feedback by "similar" users. These are people who are socially related to the searcher and may have created, viewed, or commented the content being searched. Some of today's existing social search services are offered by Internet giants like Google (Google Social Search[497] and "Search plus Your World"[498]) and Microsoft (U Rank[499]). Others are community-driven e.g. Eurekster Swiki (www.eurekster.com), Mahalo (www.mahalo.com), Wikia (answers.wikia.com/wiki/Wikianswers), Yoople! (http://www.yoople.net) and Yacy: decentralized web search (http://yacy.net/en/Applications.html).

Most personalized social search engines have been designed based on the idea that already publicly available social details about users can be leveraged without (further) compromising the user's privacy. Consequently, they provide only primitive privacy protection (e.g. features for private searches or to delete existing search logs,) if at all.

Moreover, it has been suggested that prominent social search services like Google's "Search plus Your World"[500] are not providing users with a genuine choice about their exposure to the offerings. Indeed, users of the Google search engine for instance have to opt out of seeing the results of their personalized social search. However, they still cannot opt out of having information about them (e.g. those available in Google+ - Google's social network) being accessible/found through Google search. Some legal experts and privacy advocacy groups claim that requiring users to opt out restrains individual autonomy, does not qualify as explicit consent, and may therefore violate European data protection laws.

4.2.2 PERSONALIZED E-COMMERCE APPLICATIONS

The success of the Internet coupled with new developments in ubiquitous and pervasive computing technologies have played a part in the fundamental changes in the way commercial transactions are conducted today, making E-commerce one of the top web-based applications for the foreseeable future

An increasing number of businesses and customers are eager to leverage the advantages of such technologies when engaging in business relationships with each other. Global players as well as small and medium-sized enterprises are increasing their online presence by running an ever-growing portion of their business online. Manufacturers that traditionally sell exclusively to vendors can now interact directly, via web shops, with end consumers. Some, previously non-existing vendors even operate exclusively online. This enables them to operate their businesses around the clock and to be accessible by customers and suppliers

495 Smyth/Coyle/Briggs 2011.
496 David/Zwerdling/Guy/Ofek-Koifman/Har'el/Ronen/Uziel/Yogev/Chernov 2009.
497 http://insidesearch.blogspot.de/2011/05/social-search-goes-global.html
498 http://www.google.com/insidesearch/plus.html
499 http://research.microsoft.com/en-us/projects/urank/
500 http://www.google.com/insidesearch/plus.html

dispersed around the world. According to Forrester Research, online retail sales in Western Europe are expected to grow to €114 billion by 2014, up from €68 billion in 2009.[501] In 2010, the total E-commerce market in Germany reached £33.2 billion (€39.2 billion).[502] Driving factors behind such a robust growth include the development and diffusion of broadband, high-speed Internet and a more IT-aware population. It is expected that, by 2013 almost half of Europeans will participate in E-commerce, up from 21% in 2006.[503]

As a modern business paradigm, E-commerce is intended to addresses the needs of companies to extend their potential market shares while cutting running costs and maximizing consumers' benefits (e.g. lower prizes, 24/7 access to the store).

In terms of definition, E-commerce can be seen as the set of different types of commercial activities that can be conducted electronically on the Internet.[504,505,506,498] From a business entity's viewpoint, E-commerce activities can be classified into two key groups: Business-to-Business E-commerce (B2B) and Business-to-Consumer E-commerce (B2C) activities respectively. While B2B captures the set of activities related to the management of business interactions between business entities, B2C describes the interactions between enterprise and end customers. In the past few years, a new form of E-commerce has emerged, consumer-to-consumer (C2C) e-commerce. C2C E-commerce describes commercial interactions between end consumers through some third party online platforms. Examples of such platforms include those provided by E-commerce giants such as eBay and Amazon.

One of the fastest growing segments in E-commerce is mobile E-commerce (M-commerce).[507] As reported in the Computer Woche Online magazine, analysts from the research firm Gartner Inc. are predicting a shift from E-commerce to M-commerce with a tipping point by 2015.[508] According to the same source, online retailers will have already started offering "[...] context-aware, mobile-shopping solutions as part of their overall web sales offerings." at that point. This trend is due in part to technological advances in the field of ubiquitous and pervasive computing technologies. Indeed, typical M-commerce platforms and services rely on wireless communication standards and mobile devices that provide users the ability to conduct E-commerce-related activities from anywhere, at any time. Those technological advances also offer a great opportunity to apply personalization methods and techniques to E-commerce process and activities. According to eMarketer (a site dedicated to marketing research online), M-commerce Sales in the US are expected to rise 73.1% to $11.6 billion in 2012 (91% Growth and $6.7 Billion value in 2011) and will more than quadruple again by 2015.[509]

As a key aspect of modern E-commerce strategies, personalization of M-commerce offerings allow E-commerce companies to engage with customers on a one-to-one basis while taking into account mobility aspects (e.g. current context) to support E-commerce experience. For personalization of E-commerce services, fine grained information about the users' online identities, the content of their transactions, their devices, and context of service usages have to be frequently collected and processed, and in some cases shared with third party service providers, or other users.

501 Western European Online Retail Forecast, 2009 To 2014, Forrester Research, 2010. http://www.forrester.com/Western+European+Online+-Retail+Forecast+2009+To+2014/fulltext/-/E-RES56543?objectid=RES56543
502 CRR 2011.
503 nVision 2008.
504 Zwass 1996.
505 Adolphs/Winkelmann 2010.
506 Goy/Ardissono/Petrone 2007.
507 Tarasewich/Nickerson/Warkentin 2002.
508 Computerwoche 2011.
509 E-Marketer 2011.

M-commerce activities encompass various business processes ranging from those related to online shopping, online payment, and online banking, to marketing activities such as (targeted) online advertising, product recommendation, and include trust in bootstrapping between customers, vendors, and suppliers. In each of these activities, especially those enabling personalization, sensitive data is gathered from which details about the end consumer's identity, her devices, context of service usage and habits can be inferred.

In this context, a frequent collection and processing, and in some cases sharing of information with third party service providers, has to be taken into account. Thus, (personalized) M-commerce services come at a cost. Indeed the collection and processing of sensitive customer data on M-commerce can potentially lead to a privacy breach, by revealing customers' credit card information, account balances, credit limits, home addresses (e.g. due to breaches of the customers' databases), enabling wide-range tracking and monitoring of users' online commercial activities (e.g. based on cookies), and exposing customers to spam and identity or credit card theft.

Online Targeted Advertising

Online advertising involves activities and processes related to advertising brands over the web. Online advertising is one of the major revenue-generating models in today's growing digital economy.[510,511,512] According to the Interactive Advertising Bureau, Internet advertising spending, for the year ending December 2010, grew in Europe at a rate of 15.3% and had a combined value of €17.7 billion (€15.3 billion in 2009, €12.9 billion in 2008). The US market totalled €19.6 billion and experienced a 15% growth rate for the same period.[513]

Given the competitive nature of today's online economy, advertisers and Internet companies are increasingly interested in methods and techniques that would allow them to attract and retain customers' attention, and to convince them to consume their offerings. Similar to the situation in offline world, companies hope through online advertising to increase both their customer bases and their revenues. One form of online advertising being increasing practiced on the web is known as Behavioral Ad targeting.[514,515] Behavioural Ad targeting also called Online Targeted Advertising (OTA) has great potential since it provides an easy and effective way for advertisements to be closely aligned to the interests of any individual users interacting with the system. Indeed, OTA refers to a modern form of marketing involving individuals being tracked across non-affiliate Web sites in order to monitor their online browsing behaviours and subsequently infer their preferences and interests. The information gathered is then used to decide on advertisements that should be exposed to that particular user. In recent years, a new form of OTA is gaining great market attraction- mobile or location-based advertising.[516,517] This trend is driven by advertisers' interest in leveraging the popularity of smart communication devices (e.g. smartphones, tablet), apps and wireless Internet to provide new online advertising services that take mobile user contexts and location into account.

An example of flow in a typical OTA system model could be as follows:[518,519] An *advertiser* willing to start an online campaign, i.e. to have its ads appear on certain websites, has to engage with an Ad network. The *Ad network* serves as the intermediary between advertisers and websites. It collects ads from different advertisers and embeds them

510 IAB PWC 2011.
511 IAB Europe 2010, IAB Europe 2011.
512 IAB PWC 2011.
513 IAB Europe 2010; IAB Europe 2011.
514 FTC 2009.
515 Self-Regulatory Principles for Online Behavioral Advertising, http://www.iab.net/public_policy/behavioral-advertisingprinciples
516 Gartner 2009.
517 Vega 2011.
518 Toubiana/Narayanan/Boneh /Nissenbaum/Barocas 2010.
519 Vratonjic /Manshaei /Raya/Hubaux 2010.

into web pages according to the advertisers' predefined criteria. Those websites belongs to a *publisher* with whom the Ad network has a business relationship. Terms of that relationship allow the ad network to embed technologies on the websites that would help them track their users' online activities. An internet user visiting one of the publisher websites will be automatically connected to an ad server belonging to the ad network. The ad server then selects, tailors and delivers the advertisement according to the user preference profile. The underlying business model allows the ad network to be paid on a per click basis, i.e., for each customer-generated click that directs her browser to the advertised domain/product/web store. The generated revenues are shared between the ad network and the publisher.

Unfortunately, because online advertising methods are predicated on behavioural tracking various privacy concerns come into play.[520] Specifically, cookies and deep packet inspection at Internet Service Providers (ISP) which are the most prominent techniques to keep track of users' browsing behaviours, do not sufficiently support users' control over the gathering, processing, and downstream use of their data. Indeed these tracking techniques do not solely enable the capture of information needed to tailor ad delivery to users' preferences. They can also be misused to access users' browsing details (e.g. by placing cookies on users' devices without their knowledge or consent), to track users across the Web even on sensitive sites such as health forums, and to re-construct the users' online activities with a fairly high accuracy. This could result in users being profiled or bombarded with unsolicited ads (also known as spam).

Automated Product Recommendations

On today's web, recommender engines have become fundamental tools for online marketing.[521,522,523] Many commercial websites rely on recommender engines to help customers locate and select products and contents that are likely to match their individual tastes. For instance, when surfing the web, people may receive, for example, video recommendations from YouTube, product suggestions from Amazon, and hotel reviews from TripAdvisor. In each of these cases, recommendations are generated based on the website's knowledge of the user's browsing and purchase history, interest profile, geographic information, etc. In addition, customers can use the recommender system to share their opinions and preferences for certain items with peers on the E-commerce platform.

The recommendations a website provides can be abstractly categorized as follows:[524]

- User-to-item recommendations, when the recommendation system suggests items to a user based on its knowledge of the user's behavior;
- User-to-user recommendations, when the system's suggestions aid the user in finding peers;
- Item-to-item recommendations, when for a given item, similar items are suggested and;
- Item-to-user recommendations when the system recommends users based on their association with a given item.

However, websites tend to provide more than one type of recommendation, according to the underlying business model. One common form of recommendation system is the collaborative recommendation system.[525] Two other traditional approaches for making recommendations are content-based recommendation methods (items similar to the ones the user liked in the past would be recommended) and hybrid recommendation approach (a combination of collaborative and content-based techniques). With collaborative

520 FTC 2000.
521 Resnick/Varian 1997.
522 Badrul/Karypis/Konstan/Riedl 2000.
523 Adomavicius/Tuzhilin 2005.
524 Calandrino/Kilzer/Narayanan/Felten/Shmatikov 2011.
525 Breese /Heckerman/Kadie 1998.

recommendation systems, the user is recommended items that other people with "similar" tastes and preferences liked in the past. As the name suggests, collaborative recommendation systems uses collaborative filtering algorithms to find correlations between users' interest profiles based on their browsing and buying history: relevant recommendations are derived from large-scale aggregated inputs (i.e. ratings of products or services) from multiple users. The recommendations are "anonymized" and visible to any user with a similar profile/preferences.[526] Typically, the technical implementation relies on the hypothesis that recommendation to a single user (in order to match her current interest) can be "accurately" predicted from both her preferences in the past and the preferences of similar users to her.

However, despite their success, (personalized) recommender systems are generally viewed as potential sources of privacy risk, as the user-related information needed to provide accurate / personalized recommendations is often considered sensitive. The privacy concerns that recommender systems, especially the collaborative recommendation systems, introduce are very similar to those (previously) existing in statistical database settings – how to handle a single user's raw preferences? How to ensure provable privacy guarantee when aggregating customers' preferences and disclosing them to a similar user or even the greater public? How to deal with customers who rated only a few items and thus building a smaller anonymity set? More generally, the E-commerce operators' need to share customers' recommendation databases with third parties, e.g. partners, consultants or auditors could be catastrophic from a privacy perspective. Indeed the disclosure of aggregate statistics about users' item preferences can be exploited to extract fine-grained information about that particular user.[527,528,529] As demonstrated by Narayanan and Shmatikov,[530] a seemingly anonymized and publicly available recommendation database can be easily de-anonymized resulting in a significant number of subscribers being re-identified. For their attack, the authors used the 2006 Netflix Prize data set (an "anonymized" data set of movie recommendations) which Netflix has released to improve their movie recommendation algorithm.[531] By cross-linking the Netflix movie rating data with some publicly available dataset of movie ratings on IMDb, Narayanan and Shmatikov were able to uniquely re-identify about 96% subscribers who have rated movies. More recent work have shown that a malicious user, or a coalition thereof, can successfully make inferences about someone else's input based on their faked own input.[532,533] A typical adversary can indeed use the "anonymized" recommendation records in conjunction with other data sources to uncover others' identities and to reconstruct some of their personal/intimate details. Note that this kind of attack is even easier to perform when the targets are users with rare interests, i.e. who have rated only a few products across types and domains in the systems.

In order to improve the accuracy of the recommendations, especially when it is difficult to find similarities between users who rated only a few items, both academia and industry are increasingly interested in a new approach to recommendations known as Personalized Social Recommendation.[534,535,536] The underlying idea here is to mimic offline

526 McSherry /Mironov 2009.
527 Calandrino/Kilzer/Narayanan/Felten/Shmatikov 2011.
528 Ramakrishnan/Keller/Mirza/Grama/Karypis 2001.
529 Narayanan/Shmatikov 2008.
530 Narayanan/Shmatikov 2008.
531 Netflix Netflix, Inc. The Netflix Prize Rules, http://www.netflixprize.com//rules
532 Narayanan/Shmatikov 2008.
533 Calandrino/Kilzer/Narayanan/Felten/Shmatikov 2011.
534 Geyer/Freyne/Mobasher/Anand/Dugan 2010.
535 Ma/Zhou/Lyu/King 2011.
536 Machanavajjhala/Korolova/Sarma 2011.

social recommendations e.g. the recommendation for a book or movie we receive from people we trust. The hope being that, new recommendation algorithms that leverage social trust relationships existing among users as well as other personal information available on public forums and other social networks would generate recommendations that are more accurate.

On the other side of the coin, privacy concerns are inescapable when social network sites are mined and the personal information collected is shared with third parties that make recommendations.[537] The main concern is about possible leakage of information regarding the existence of edges (i.e. social ties between users) between specific nodes in the social network. This information released could include the entire shopping history of a specific user or details about the existence, or lack thereof, and strength of social ties and trust between two users. This would constitute a privacy breach for many users.

4.2.3 ONLINE SOCIAL NETWORKS

The emergence and widespread popularity of social networks on the Internet is changing the way we live and work.

Recent reports from the market research company Nielsen [[538]][[539]] indicate that social networking and blogging are now the most popular activities on the Internet worldwide,[540] accounting for the majority of time spent online and reaching at least 60% of the active Internet population. In Germany, Internet users spend more time on these networks than they do on any other Website categories, a total of 12.7 Billion minutes during May 2011, according to the Nielsen's Social Media Report-Q3 2011.[541] Nielsen's figures were recently backed up by a new report from the German Federal Association for Information Technology, Telecommunications and New Media (BITKOM) that said 74% of German Internet users are members of at least one online social community: most of them (66%) are active users, 59% are daily active users.[542] In another report, Nielsen points out that three of the world's most popular brands online are social-media related.[543] One of them, Facebook, is the current leading online social network and claims to have more than half a billion of users actively using its platforms, and billions of pieces of contents (including web links, news stories, blog posts, notes, photo albums and videos) uploaded on it each month.[544] Another one, Google+, Facebook's primary rival social networking site, has reached 62 million registered users and predicts 293 million users by the end of 2012.[545] The prospects for the online social networks sector look very healthy over the next few years. According to one of the latest E-Marketer's report, the combined number of social network users in France, Germany, Italy and Spain will climb from 100.1 million in 2011 to 141,9 million in 2015.[546]

This development motivates the emergence of a broad variety of online services. Individuals and organizations are increasingly reliant on online social networks (OSNs) to construct and manage their digital representations and reputations. Individuals use OSNs to establish, maintain, and revoke online

537 Machanavajjhala/Korolova/Sarma 2011.
538 Nielsen 2011.
539 Nielsen 2009.
540 In the report, the terms 'Global' or 'World' encompass the USA, Brazil, United Kingdom, France, Germany, Italy, Spain, Switzerland, Australia and Japan. Those are countries in which Nielsen Online has a NetView panel.
541 Nielsen 2011.
542 Huth/Arns/Budde 2011.
543 Nielsen 2010.
544 http://www.facebook.com/press/info.php?statistics
545 https://plus.google.com/117388252776312694644/posts/ZcPA5ztMZaj
546 http://www.emarketer.com/blog/index.php/tag/social-network-usage/

relationships with old and new acquaintances, colleagues, friends and family members. In addition to benefiting individuals, i.e. enabling them to create and manage their own online communities, OSNs have significant business value for organizations. Public and private organizations increasingly rely on OSNs as an integrated medium for marketing and public relations.[547] Most of them use these networks to enrich their underlying online offerings, making them more attractive to online users, and ensuring a direct and regular engagement with (prospective) customers. Others use OSNs as recruitment and screening tools.[548,549] Recently, we have also been witnessing a growing use of OSNs in the political space. In fact, citizens across the globe are increasingly using OSNs to engage in political activities, from exchanging views with others, signing up as "fan" of a candidate, to discovering contacts' political interests or affiliations, and organizing social movements and protests.[550,551]

Definition and Main Characteristics

According to boyd and Ellison OSNs are "web-based services that allow individuals to (i) construct a public or semi-public profile within a bounded system; (ii) articulate a list of other users with whom they share a connection, and; (iii) view and traverse their list of connections and those made by others within the system".[552]

Based on the above definition, common characteristics of OSNs are that they provide users the ability to create a virtual personal space containing an online profile; to keep their online profile updated; and create relationships with others based on common interests, such as games or health issues. Moreover, OSN users can browse through their contacts' profiles and upload multimedia contents, post messages, and annotate published content with tags, reviews, comments, and recommendations. A user profile, usually set up when the user signs up to the OSN platform, contains information such as the user's first and last name, gender, date of birth, relationship status, education and work information, details about political and religious views, photos, and other information.

OSN users can tag other people who appear in content when posting that content into their own virtual space, the spaces belonging to people with whom they have a relationship, or into public pages. As a matter of fact, each tag is an unambiguous reference that links to another user's profile. As a result, a social graph containing a large set of references to various kinds of users' related information including user profiles, the related social connections and trust relationships, and users' interactions within the social network, begins to emerge. By providing means for users to manage their social and trust relationships, OSNs allow individuals or groups to specify policies to regulate access to profile data and friend lists, or communication with other users. Note that "friend" is a term typically used in relation with OSNs such as Facebook, Google+, and Myspace to describe OSN users with whom the owner of an account is connected. Depending of the purpose of the OSN, contacts are often termed differently, e.g. as "followers" on Twitter (https://twitter.com/) or "subscribers" on Youtube (www.youtube.com).

Social Networking Data

To participate in OSNs, i.e., interact and communicate with others, users have to share a variety of identity-related information and attributes. According to Schneier,[553] this includes:

– *Service data* which is the data the OSN platform requires the users to reveal in order to participate in the

547 Deloitte 2011.
548 Davison/Maraist/Bing 2011.
549 Langheinrich/Karjoth 2011.
550 Zeh 2011.
551 Lotan/Graeff/Ananny/Gaffney/Pearce/boyd 2011.
552 boyd/Ellison 2007.
553 Schneier 2010.

network. Such data might include the user's profile attributes (e.g. user's identity attributes, her social and trust relationships to other member of the virtual community, and preferences) and login credentials (username and password).
- *Disclosed data* is the set of contents that a user uploads on her own OSN profile. This includes messages, comments, blog entries, photographs, video, and so on.
- *Entrusted data* which is the set of all data objects a user posts on other users' pages. In contrary to disclosed data, user cannot enforce privacy control over entrusted data once she posts it.
- *Incidental data* which is data that any other member of the OSN reveals about the user. This includes tagged video of the user uploaded by someone else, or blog entry about the user but written by somebody else.
- *Behavioural data* refers to what the OSN site collects about users' interactions and activities in relation to their use of the OSN services. It typically includes the user's browsing history along with other details such as the list of topics the user has commented/written on, the profiles the user had visited, the frequency and duration of use of certain service (online games) and so on.
- *Derived data* which is the set of user-related data that can be inferred from all the other types of data. For example, user political views can be deduced from the aggregation of information such as her most frequent comments on political topics, her location history, and unconcealed information about her friendships.

Another way to look at social networking data is to classify data according to the view of an OSN as a direct graph in which nodes represent individual users in the OSN, while edges represent social links between the users. Here, user-related social networking data include three types of data:[554,555]

- *Identity data* which describes who the user is in the social network. It includes identity and profile attributes, and privacy policies managed at corresponding nodes.
- *Content data*. The collection of content that was generated and/or uploaded by OSN users. Examples of content data include messages, photos, videos, and all other data objects created through various Social Web activities.
- *Social-graph data*. It represents who, and to which degree, the user knows or is linked to in the social network. It includes her social and trust relationships.

Online Social Networks System Architectures

From a system architecture viewpoint, there are two ways of implementing OSNs, centralized and distributed model respectively.

- *Centralized OSN Architecture Model*: Here, the central OSN operator offers key functionalities such as data storage, service access or network monitoring and maintenance. Today, most OSNs rely on a centralized data model. This is in part because client-server systems are straightforward, easy to deploy and maintain, and enable commercial OSN providers such as Facebook, Google, LinkedIn, and StudiVz to control access to, and activities within, the OSNs. Furthermore, a centralized architecture model enables the OSN provider to maintain and manage all relevant data under a single administrative domain. However, the centralized OSN model raises concerns with regard to the single point of failure character of OSN operator, and the ability of the central OSN operator to meaningfully enforce users' privacy requirements.
- *Decentralized OSN Architecture Model*: In this model, users' social networking data are stored and maintained across multiple administrative domains. The trend is to design next-generation OSNs according to this model, adopting the peer-to-peer (P2P) paradigm to realize the collaboration and information sharing between

554 Ko/Cheek /Shehab/Sandhu 2010.
555 Hu/Ahn 2011.

the OSNs peers. OSNs peers are independent parties who are not only users of the OSN but also host application servers and thus making OSN resources available so that other members may use them. The main advantage of decentralized OSN architecture models to avoiding a central entity that may perform abusive data retention and mining. In addition, enabling peers to host personal data is viewed as more privacy-preserving than relying on a central entity to enforce peers' privacy requirements. From an operator perspective, relying on a P2P model is cheaper than deploying and managing a purely centralized platform. However, today's existing decentralized OSNs, e.g. Diaspora[556], PeerSon[557] and Safebook[558], still suffer from drawbacks of p2p-based systems. For instance, the lack of centralized control entity makes it difficult for decentralized OSNs users to assess and control the behaviour of their peers, making trust management in that setting a challenging issue.

OSNs can also differ both in target and in scope, allowing further differentiating between entertainment- and business-dedicated OSNs, respectively. Examples of OSNs that are dedicated to providing news and entertainment services include popular platforms such as Facebook, Google+, Twitter, Flickr and Hi5. Their focus is on delivering fun and interactive social experiences, including collaborative gaming, content recommendation, dating, etc.Business- dedicated OSNs (or professional OSNs) on the other hand aim to connect professionals around common business and professional interests. In addition to displaying a brief summary of the user's professional expertise, accomplishments and contact details, a typical professional user profile also contain basic information (names, job title) and other personal information (marital status and date of birth). Popular examples of professional OSNs are LinkedIn (www.linkedin.com), Xing (www.xing.com), Ecademy (www.ecademy.com/).

Privacy Concerns in Online Social Networks

As the popularity of social networks expands and the amount and type of personal data that can be processed within, and exported from, those networks increases, concerns related to the possibility of users' privacy rights being weakened or eliminated due to unintended or malicious actions increase as well. If realized, such an action (which is a threat to users' privacy) can have undesirable, damaging and even life-threatening consequences for individuals.

Indeed, OSNs entail potentially significant privacy risks for individuals participating in such networks. Some information disclosed by users in their profiles (e.g. real name, date of birth, home address, sexual/religious views, phone number, social relations, etc.) is of a very private nature. Users participating in OSNs are not only able to seamlessly share their preferences, current activities, thoughts, and self-generated multimedia contents, but they can also reveal sensitive details about any other network participant with whom they have a relationship. In most OSNs, the OSN operator stores information contained in users' profiles as well as the details about the relationships between users centrally. Moreover, the increasing integration of OSNs with third party personalized services (e.g. location-based services) may come with new threats to users' privacy. More specifically, the availability/accessibility of users' related social networking data inside and outside their respective online communities may facilitate exposure to personalized spamming and online risks such as social phishing, identity theft, online scam, stalking, and cyber bullying along with all the legal and financial consequences.[559,560] Furthermore, the misuse or unintended disclosure of user personal data may lead to embarrassment and loss of reputation and credibility among friends, colleagues, and business partners.

556 Diaspora, https://joindiaspora.com/
557 Buchegger/Schiöberg/Vu/Datta 2009.
558 Cutillo/Molva/Strufe 2009.
559 Tuffield 2007.
560 Jagatic/Johnson/Jakobsson/Menczer 2007.

In general, two major types/categories of threats to privacy in OSNs can be distinguished: threats associated with the availability and accessibility of user data within OSNs, and those related to the disclosure of personal information to third-party applications, advertisers and other aggregators outside the boundaries of the OSNs.[561,562,563]

The first type of threats comes from i) users revealing too much private information to other users within the network; ii) and the operator's ability to centrally store all kind of social networking data available on its platform. OSN users tend to believe that only a restricted group of individuals, their contacts, can access their personal information. In fact, this information can be accessed by other entities involved in the OSN, i.e. fellow OSN users, the operator, advertisers, third party application providers, external data aggregators, etc. When participating in OSNs, users reveal personal information either while being unaware or unconcerned with their actions and/or the consequences those could entail. This is partly due to the difficulty for the user to fully understand the operator's privacy policies[564] and the lack of usability of, and in some cases design flaws in, privacy settings in those sites[565,566,567,568,569].

Threats resulting from those limitations include strangers' ability to view the user's supposedly private data, and the possibility that any OSN participants can divulge information about somebody else, in some cases without the consent or knowledge of that person. Indeed, the possibility for OSN users' to tag images they upload with some meta-data, e.g. links to profiles of persons on the photo, date of creation, may facilitate an inappropriate flow of information from one social context (cf. [570]) to another resulting in an unintended leak of intimate details about a person's life. In offline world, this could lead to embarrassment (e.g. user's unflattering photos, posted on a friend's page can be accessible to and de-contextualized by others), damage to someone's career and reputation, and in some cases financial loss. A few years ago, a student teacher was denied a teaching degree following the disclosure of a „drunken pirate" photo of her on an OSN site.[571,572] More recently, two British tourists were detained, kept locked in a holding cell for 12 hours at a U.S. airport and then denied access to the U.S. on grounds of security risks. Agents of the Department of Homeland Security asserted that their post on Twitter about "destroying America"[573] is evidence that both tourists have planned to commit crimes in the U.S.[574] In addition, there are evident risks to individuals and organizations through careless use of OSNs. For instance, burglars may use these networks to discover users' personal details such as residential address and living standard, monitor profile updates of the intended victim (e.g. looking for posts like "I'm on vacation in Paris until February 31!") and break into properties that have been left vacant. Moreover, if someone'saccount

561 Krishnamurthy/Wills 2008.
562 Gross/Acquisti 2005.
563 ENISA 2007.
564 FTC 2010.
565 Madejski/Johnson/Bellovin 2011.
566 Hill 2011.
567 Besmer/Watson/Lipford 2010.
568 McDonald/Cranor 2008.
569 Hull/Lipford/Latulipe 2011.
570 Nissenbaum 2010.
571 UscourtsNo.07-1660 2008.
572 Rosen 2010.
573 "Destroy" is a British slang for "party"
574 US bars friends over Twitter joke, The Sun, 30 Jan 2012 http://www.thesun.co.uk/sol/homepage/news/4095372/Twitter-news-US-bars-friends-over-Twitter-joke.html

has been compromised, the consequences to them and to those in their network may be severe both in trust and financial terms. That is, attackers who have gained access to a user account (as result of an identity theft attack) may exploit the opportunity for socially engineered scams targeting the victim's online "friends". Unfortunately, due to a pre-existing trust relationship with the owner of a compromised account, intended victims of online scams are more willing to accept unsolicited business propositions (e.g. "*I have won a Microsoft lottery, … , but need to pay for postage and handling. Please send me money*") from that friend than one from a total stranger. This type of threat can also be facilitated by the fact that some social network sites only provide weak registration and identity verification methods. The security weaknesses in the registration and identity verification methods also allow a malicious user to create a (large number of) fake user accounts and take advantage of the (good) reputations and privileges associated with these accounts to mislead other users.[575] Furthermore, the security weaknesses in the registration and identity verification methods can also be exploited for attacks such as Sybil attacks.[576]

There are also concerns that OSNs can be used as settings for gathering information that employees share online to facilitate many other crimes including industrial espionage and cyber attacks on employers.[577,578,579] However, even if the user decides to share less and make her profile only accessible to a very restricted network of friends, and thus assumes concealment of the majority of her private attributes, it is still possible for an adversary to gain knowledge of those attributes by correlating public details about the targeted user's group affiliations and friend lists.[580] The underlying assumption of this kind of attacks is that users who are members of the same social groups also often share similar cultural and social attributes. The social context information can then be used by attackers to infer more private information.

As previously stated, beyond revealing private information to other users within the OSN, another potential source of privacy threats is the operator's ability to collect and mine huge amounts of user-related data, including users' identity attributes, blog entries, comments sent and received, photos, device's IP-address, and browsing history. Accordantly, the OSN can be considered as a central repository of users' data to which a single OSN operator, and in some instances third parties, have unlimited access. Such large-scale data retention may infringe on users privacy and ultimately undermine consumers' trust and confidence in the OSN operator.

Moreover, the OSN operator may decide to change/update its privacy policy (part of its terms of service) without giving its members proper notice and obtaining users' explicit consent before the modifications. For instance, recent privacy policy changes by prominent OSNs have been opt-out, meaning that the user agrees by default. These changes are typically not to the advantage of the members. Removing restrictions in order to enable a broader usage of individuals' data, i.e., granting the operator the permission to use individuals' personal information (e.g. name and picture) for secondary purposes like advertisements, or transferring all ownership rights of personal data and content to the operator. The controversies over the Facebook decision in 2009 and 2011 to modify its

575 Twitter's identity verification process recently came under scrutiny after Wendi Deng, the wife of News Corp. Chairman and CEO Rupert Murdoch, had a fake Twitter account set up in her name. Twitter first labeled the fake account as genuine before subsequently removing it. http://www.guardian.co.uk/media/2012/jan/03/wendi-deng-twitter-account-fake

576 Douceur 2002.

577 Dumitru 2009.

578 Davison/Maraist/Bing 2011.

579 Langheinrich/Karjoth 2010.

580 Zheleva/Getoor 2009.

privacy policy[581,582,583] and LinkedIn's latest change in its terms of use[584,585] illustrate this.

Indeed, OSN operators may decide to use the personal information collected for purposes and in contexts different from the ones initially considered by the data subject (i.e. user). There is a great deal of evidence[586] that personal information revealed on OSNs has been shared (possibly without users' knowledge) with third parties who use it for targeted advertising, discrimination (e.g. price discrimination), etc. Moreover, ensuring that sensitive data cannot be retrieved beyond a specified time is, in many of today's popular OSNs, not a practical expectation. This is particularly problematic when the user wishes to delete her account from the OSN, including secondary information such as her public comments and photo albums. Even if users' personal data were to be deleted from the operator's servers, Internet caches and other community backups will continue to host copies of the sensitive data making them still publicly accessible.[587]

From an attacker's viewpoint, social network data is a high-value target, as it is considered by most operators to be a financial asset. An internal attacker (e.g. an OSN's employee) may access the provider's database and extract information about the identities, contacts, and online activities of a large set of users. External attackers may break into the operator's database, which may lead to embarrassment e.g., exposure of user's intimate information to the greater public. The attackers may, in either scenario, do this out of curiosity or with the intent to harm the user e.g., using the data for identity fraud, online scams, cyber bullying, or even off-/ online stalking. Hence, without restrictive access to the OSN user databases, and trust between users and the operator, privacy threats would be ever-present with regard to the confidentiality and proper handling of user data stored on the operator's side.

The second category of privacy threats emerges from the pervasive tracking of users' activities and interactions by third-party applications and data aggregators. Most of today's OSNs allow users to install third party applications (or "apps") such as online games and media plugins. Once installed, these apps may need access to various types of personal data, depending on the functionalities they are expected to offer. The way in which users' private information is gathered and further processed by third-party applications is rarely transparent to the users, raising questions about the privacy implications of the services. Furthermore, there is no reason to believe that these apps are designed with privacy in mind. In fact there have been reports of privacy breaches due to poorly designed and implemented apps.[588,589] For instance, Balachander and Wills[590,591] have discussed the pervasive and inescapable tracking of OSN users' actions by third-party advertisers and data aggregators, describing how details from the HTTP header and cookies sent by apps lead to exposure of the user's identity and the disclosure of her friends' private attributes.

Despite privacy concerns expressed by advocacy groups, consumers and regulators, the sharing of social graph data

581 The Electronic Privacy Information Center, Facebook Privacy, http://epic.org/privacy/facebook/
582 Vascellaro 2009.
583 Walters 2009.
584 Schoemaker 2011.
585 Raice 2011.
586 F.T.C. Charges Myspace With Breaking U.S. Law in Sharing Users' Personal Information http://www.nytimes.com/2012/05/09/technology/myspace-agrees-to-privacy-controls.html
587 Vaas 2012.
588 Egele/Moser/Kruegel/Kirda 2011.
589 Recently detected features of the social networking app Path allow access and upload of users' address book details without user's knowledge and consent. http://mclov.in/2012/02/08/path-uploads-your-entire-address-book-to-their-servers.html
590 Krishnamurthy/Wills 2009.
591 Krishnamurthy/Wills 2010.

with third parties (e.g. marketers, application developers, and academics) remains the foundation of the current business model for many OSN operators. The social graph, or part of it, is what the OSN operator sells to or shares with third parties. While advertisers would use this data to extract possible profitable patterns and mine valuable market information, academics, e.g. social and cultural researchers, may analyse it to study patterns in human behaviour in OSN sites and the interplay between online and offline social phenomenon. However, once third parties obtain access to users' personal data, they, not the users, typically have actual control over how to further use or share it.

In addition to privacy risks posed by the use of third party applications, the fact that most people have multiple OSN accounts poses a significant challenge to the user privacy. These different OSN accounts contain details about different aspects of their lives and aggregating these details is a trivial task. As demonstrated by various researchers,[592,593] an attacker (e.g. a data aggregator like Spokeo)[594] may be able to merge and correlate disparate pieces of information about user's profiles from different OSNs to generate a more or less complete set of online identity attributes of that specific user. The authors refer to such a set as the user's "*social footprint*". A user's social footprint may be used by third-party servers and data aggregators to monitor the target's activities and interactions across different OSNs and over extended periods of time, even if the latter registered with different social network identifiers. More recently, Acquisti et al. demonstrated, relying on a similar method, the feasibility of re-identifying individuals online and offline, using information collected from different publicly available data sources.[595] In a test, the scientists compared 277.978 Facebook profiles against 6000 profiles extracted from an online dating Web platform. They were able to match 1 in 10 members of the dating site (all members' profiles were pseudo-anonymized by default) with their real names from the social network platform Facebook.

Another aspect of the (re-) identification threat the OSN users are facing comes from the possible release of social network data to third parties, e.g. academics, government entities. These entities may receive the data either as a complete OSN graph or as part of it. Prior to the release, the OSN operator is obliged according to existing legal frameworks to anonymize and sanitize the OSN graph in order to avoid an a-posteriori re-identification by attackers. However, recent work by Narayanan et al. demonstrated that existing approaches to anonymized social graphs do not work on "realistic" networks.[596,597] They showed that sensitive information about specific persons can be extracted from anonymized OSN graphs with a relatively high success rate. Their underlying threat model assumes an attacker not only having access to the (sub-) graph being released, but also to publicly available auxiliary information such as the links between users and details about another network in which users' memberships may overlap with those in the target network. Wondracek et al. have recently presented a similar attack.[598] The authors demonstrated that a particular user in an anonymized OSN can be re-identified with high certainty, based on her publicly available group membership attributes on other social networking sites.

As the impact and number of features provided by OSNs continue to grow, organisations including business and government entities are looking increasingly at OSNs as a medium with the potential to aid the improvement, work processes, collaboration and knowledge management between otherwise disconnected groups of

592 Irani/Webb/Li/Pu 2009.
593 Irani/Webb/Li/Pu 2009.
594 www.spokeo.com/
595 Acquisti/Gross/Stutzman 2011.
596 Narayanan/Shmatikov 2009.
597 Calandrino/Kilzer/Narayanan/Felten/Shmatikov 2011.
598 Wondracek/Holz/Kirda/Kruegel 2010.

employees.[599,600,601] In addition, more and more companies are interested in exploiting the commercial and marketing opportunities OSNs offers.[529,602,603,604] Many leading companies are increasingly relying on OSNs as a medium to engage more directly with potential customers (Social Shopping).[605,606] Advertisers view OSNs as media to which one may easily propagate marketing messages, and influence the buying decision process of, a very large consumer base.[607,608] For human resource departments, OSNs have become vital and powerful recruiting tools.[609,610,611]

Social Commerce

Generally speaking, "Social Commerce" describes the use of OSNs in the context of E-commerce. From a technical standpoint, Social Commerce refers to an integration of different Web 2.0 tools such as OSN sites, widgets and E-commerce strategies aiming at providing Web users the opportunity to jointly participate in the comparing, buying, recommending, and (re-) selling of products and services online. One key driver of social commerce is the increasing use of OSNs by internet users to learn and share knowledge about new products and brands. A growing number of advertisers and online retailers nowadays are assessing ways to leverage the potential of Web 2.0 applications to improve their engagement with potential customers, hoping for increased user base and sales. By 2015, most companies will generate about 50% of Web sales via their social presence and mobile applications, according to Gartner's estimates.[612] Based on a recent Booz & Company report, the social commerce market size should grow from estimated US$5 billion in 2011 to about US$30 billion in by the end of 2015.[613]

By leveraging OSN potentials and making their entire E-commerce infrastructure social, online retailers can transform their sites into platforms where (potential) customers create communities of peers, i.e. communities in which they share experiences with, and preferences for, certain brands, products, and services.[614] Indeed, relying on their ability to upload videos, photos, and participate in forums embedded into retailers' websites, customers can share their product experiences with others and thus provide valuable information that may influence buying decisions of prospective shoppers. Nowadays, more and more (E-commerce) sites have started assessing ways to leverage OSN profile information of potential customers to deliver individualized shopping experiences from their OSN sites. A widespread approach to achievement of this goal is the integration of social plug-ins such as Like buttons and Wish Lists into traditional web sites.

In the following paragraphs, a brief introduction to the Facebook Like button and Wish Lists will be given, and possible impacts on individuals' privacy reviewed.

599 i.e. group associated with particular projects, departments or functions within the organization
600 Murphy/Salomone 2010.
601 Tomlinson/Yau/MacDonald 2010.
602 Schäfers 2008.
603 Invoke 2010.
604 Korolova 2010.
605 Schäfers 2008.
606 Invoke 2010.
607 Korolova 2010.
608 Nielsen 2009.
609 Davison/Maraist/Bing 2011.
610 Langheinrich/Karjoth 2010.
611 Dumitru 2009.
612 http://www.gartner.com/it/page.jsp?id=1826814
613 Anderson/Brusa/Price/Jerell/Jo 2011
614 Schäfers 2008.

The Facebook Like Button

The Facebook Like button[615] is the key technology of the Facebook Open Graph initiative launched in April 2010. It is a plug-in that allows Facebook users to share their interests and preferences for a website or items displayed on that site with "friends" on Facebook. In addition, the Like button, along with other Facebook's social plug-ins such as the send button[616], the recommendation plugin[617] and the Activity Feed plugin[618], enables traditional sites to expand into the social web. According to Facebook, "the Like button lets a user share ... content with friends on Facebook".[619] Relying on the Open Graph protocol[620] and the Open Graph tags technology, the Like button tool can be included not only to Facebook, but also to any page on the Web. Typically, each Facebook Like button displayed on a third-party website is associated with a counter representing the number of Facebook users who have clicked it to express their positive feedback.

When clicking the button, the user's feedback about the website or items on the website is published back to her friends' Facebook profiles, i.e. a link to the website appears in the user's activity stream. All of that person's friends can thus see the link, click on it and visit the website if they wish. Moreover, when visiting a website that includes such a Like button, Facebook users are able to access the reviews their friends have made on items displayed on that site. The Facebook Like button can, thus, help online service providers to attract more potential customers as it gives an indication of how many "Likes" a website, a content, or a product has received.[583] For Facebook users, the Like button is personalized, i.e. it indicates what and who of their friends has visited and "Liked" the item. From an advertiser standpoint, the Like button presents numerous advantages.[621,622] One key benefit "[...] is that it lowers the psychological barrier to connecting with commercial entities on a brand's site – while previously users could „Become a Fan" of a brand, they now simply „Like" that brand's page, resulting in higher engagement. Another benefit is that it increases clicks for web publishers: Facebook users are more inclined to „Like" a news article than they are to hit a „Share" button."[623] The Like button, as important marketing instrument, gives anyone running a website the opportunity to connect the site to, and leverage, the ever-growing network of Facebook's users[624] for monetary purposes. Indeed, less than a month after its launch, more than 100.000 sites had integrated the Facebook Like button technology.[625,626,627,628] Nowadays, an ever growing number of organizations have the Like button included on their web sites.

However, despite all the benefits of the Like button and other Facebook social plug-ins in terms of enabler of direct engagement with web users and knowledge-based collaboration, their explosive popularity also raises concerns related to security, trust and

615 http://developers.facebook.com/docs/reference/plugins/like/
616 It allows users to easily send websites contents to their friends
617 It gives users personalized suggestions for pages on your site they might like
618 It shows Facebook users what their friends are doing on your site through likes and comments
619 http://developers.facebook.com/docs/reference/plugins/like/
620 http://developers.facebook.com/docs/opengraph/
621 Cashmore 2010.
622 Facebook 2010..
623 Cashmore 2010.
624 More than 800 million active users according to Facebook (http://www.facebook.com/press/info.php?statistics, accessed 17.12.2011)
625 Fletcher 2010.
626 Facebook 2010.
627 http://www.facebook.com/press/info.php?statistics
628 http://searchengineland.com/has-facebook-become-the-master-key-to-unlocking-the-web-75139

privacy.[629,630,631,632,633] From a technical perspective, the Facebook Like button is a piece of HTML (XFBML and Iframe) code embedded in a website. That code allows certain commands to be executed each time the website is loaded or refreshed. An example of such commands is to send third-party cookies (see Section 4.3.1) to users' browsers or to use previously installed cookies to collect and report users' related information to Facebook. The situation is aggravated by the fact that the cookie-related processes are usually non-transparent to the users. Facebook could thus use the Like button to track and profile Internet users across websites, regardless of whether they actually click on the button, log out of Facebook, or even have a Facebook account. Indeed, for non-members of the Facebook platform visiting websites that display the Like button, Facebook may be able to collect details about their respective browsing histories. This information typically includes the URLs of the visited pages, the click through rates, date/time of the visit, time on-site, the IP address of the device used, browser / OS fingerprint, etc. Assuming that the user joins the Facebook community later on using the same device, i.e. with an unchanged IP address, Facebook would be able to establish the correlation between the browsing history collected earlier and the newly created Facebook profile. In the case of Facebook users browsing the web, Facebook may theoretically be able (relying on third party cookies installed by its Like buttons) to collect details about their browsing activities and to link them to the respective Facebook accounts already containing sensitive information such as real names and dates of birth. It should be noted that even after the user has logged out, Facebook's ability to track her via cookies, i.e. to associate a certain set of browsing activities to her unchanged IP-address, remains relatively intact.[634] Clearly, the linking of internet users' browsing histories and information in their Facebook accounts can lead to a privacy breach. In addition, much of the information collected by the Like button when tracking users' activities across the web is usually done without their explicit knowledge and consent. Moreover, even if a user decides to delete sensitive information created through the use of the Like button and removed it from her profile, that information would remain visible on third party websites. On the other side of the coin, there are still controversies over the type of information collected and reported to Facebook. Another point of controversy is the potential responsibility of website owners' to assume any liability for including the Like button on their sites.[635]

Aside from the risks of permanent monitoring and tracking, the Facebook Like button's ability to propagate users' positive feedback about websites they have visited to their friends may also facilitate the launch and propagation of malware and spam. The underlying malicious technique is known as Likejacking.[636] That is, an attacker (e.g. a spammer) may exploit web browsers' vulnerabilities and Facebook's vulnerabilities to include a Like button on its innocuous-looking, yet infected website. This way, users can be tricked into liking a website or a content they did not intentionally mean to „like". This may result in victims recommending their friends to click on the rogue website/ content they have posted on their walls. Since friends in OSNs tend to trust each other, it becomes easier for hackers to create such self-propagating worms and spam. Indeed traditional email worms have being updated for the social networking age enabling them to steal personal

629 Meyer 2011.
630 ULD 2011.
631 Venzke 2011.
632 Caviglione/Coccoli 2011.
633 Fletcher 2010.
634 Mills 2011.
635 ULD 2011.
636 Sophos 2010.

data (e.g. Facebook credentials) and to spam victims' contacts on the social-network, as evidenced by increased incidents and media reports.[637,638]

Two other social plugins which are ubiquitous on the Web are the Google +1 button[639] and the tweet button[640]. While appearing to be tools to help website owners to attract more visitors, the systematic use of third party cookies onto any site willing to be part of the social Web also allows the Internet giants behind these technologies to track and profile Web users. Indeed, whenever somebody browsing the web accesses a webpage that displays a twitter button and/or a Google +1 button, the buttons (which are in fact small piece code from Twitter or Google added onto the webpage) signal back to Twitter/Google that the user have looked at that page. This happens regardless of whether the user clicked on the button or has been logged in or not. It can be assumed that user-related information other than IP address is collected since cookies are typically used to track users across websites. Similarly to the Facebook Like button, there is an ongoing controversy around the lack of user knowledge and consent (opt-in) for such a pervasive and inescapable tracking and profiling.

Wish Lists

An online Wish List provides features on E-commerce web sites allowing consumers to let others know about products and services that attract their interest, e.g. books the List owner would like to read. It helps users to keep track of items they want or search for as well as provides the ability to comment on friends' Wish Lists. Some people tend to create Wish Lists shortly before they celebrate special events, some of which have a private character, like birthday, weddings, and funerals. In addition to advantages provided to individuals, online wish list services are also benefiting vendors and retailers. The latter can collect data revealed by wish list owners from which they can then extract valuable knowledge. For instance, vendors may use the information displayed on online wish lists for predicting demand for certain products. Much like other internet services, Wish List offerings are free to users but allow Wish List providers to make money by publishing ads (their own and others') on their sites.

The more Wish List becomes popular and users share and make their preferences public, the more Wish List providers can amass huge amount of private information and sell it to third parties, in particular advertisers. As a consequence, advertisers are able to target individuals on a more granular level. Moreover, both authoritarian and democratic governments may have strong incentives (e.g. national security or online censorship and surveillance) to collect, and retain as long as possible, information about users' interests in and use of certain products (book and music) that the authorities may view as subversive. Furthermore, much of the information in online Wish Lists is not only very private by nature but also searchable and available to the greater public. This raises questions about privacy implications of online Wish List services. In 2006, Tom Owad presented a comprehensive review of such privacy implications in an article entitled "Data Mining 101: Finding Subversives with Amazon Wishlists".[641] He demonstrated the feasibility and effectiveness of re-identification attacks on online wish list services. For his attack, Owad downloaded 260,000 Amazon Wish Lists in which individuals' identities were protected by means of pseudonyms. He was able to retrieve the complete address of one of four list owners by entering the wish list names, cities, and states to the Yahoo! PeopleSearch[642] search engine. Owad's attack is an evidence that naïve anonymization of Wish Lists prevent unintended disclosure of personal information only to limited degrees.

637 Constantin 2011.
638 John 2010.
639 http://www.google.com/+1/button/
640 https://dev.twitter.com/docs/tweet-button
641 Owad 2006.
642 http://people.yahoo.com/

Mobile Online Social Networks

Another trend in the OSN domain is the phenomenon of mobile Online Social Networks (mOSNs), which describes as an extension of online social networking to mobile devices. According to the Facebook's statistics page, more than 350 million active users currently access Facebook through their mobile devices, and nearly 475 mobile operators globally deploy and promote Facebook mobile products.[643] A recent study by eMarketer forecasts a fivefold growth in the number of mobile users accessing social networks from their mobile devices, indicating a rise from 141,4 million mobile social network users in 2009 to 760,1 million by the end of 2014.[644] Backing these figures, Gartner predicts that companies will generate 50% of online sales via their social presence and mobile applications by 2015.[645]

Such a convergence between the social and mobile sphere is driven by the widespread adoption of smart mobile devices (e.g. Smartphone and tablet PC) and the explosion in mobile Internet usage. The growing public interest in and economical potentials of mobile social networking have pressured many existing OSNs to adapt and new native mobile OSNs to emerge. While the former OSNs, e.g. Facebook, have redesigned their websites, contents and access mechanisms to account for smart mobile devices limitations (e.g. limited bandwidth, small screen size, and latency), new emerging native mobile OSNs platforms are designed to explicitly take advantage of mobility and location awareness from the outset.[646,647] Examples of this new type of mOSN platforms include Google latitude (www.google.com/latitude), Loopt (https://www.loopt.com/), Foursquare (https://foursquare.com/), and Twitter (http://twitter.com/).

A common characteristic of these new types of mOSNs is that they focus specifically on mobility and awareness, allowing mobile users to share their presence and location details with "friends". Based on such context information, mOSNs provide various location-based services including the (semi-) automatic sharing of, or search for, geo-tagged contents within virtual communities, and the discovery and interaction (e.g. arranging a meeting) with "friends" who happen to be nearby. Mobile online social network services typically rely on user's location details, along with their profile information and preference history, to provide indications (e.g. via short message service) about the availability of certain contents or presence of individuals/ friends within a certain distance of her current location. While some mOSNs like Google latitude and Loopt, exclusively focus on enabling live tracking of friends on a map, other platforms e.g. Gypsii (http://www.gypsii.com/) and Foursquare also allow their users to annotate and share photo and video across the platform and through other popular OSNs such as Facebook.

Moreover, the mOSNs trend is expected to spread into, or merge with, already existing business applications/models of social networks. For instance, there is a growing number of advertisers looking to tap into the larger pool of potential customers formed by the growing number of smartphone users (427.8 million devices sold to end users worldwide during the first quarter of 2011[648] and 1.2 billion users visiting social networking sites alone in October 2011[649]) and the money from personalized mobile ad delivery. This will be facilitated by the opportunity offered by mOSNs to apply personalization and recommendation. It is expected that the integration of mOSN, personalization and recommender system technology would allow the rise of new mOSN services tailored to people's needs and interests.

Despite such a great promise, the underlying idea of mOSNs, i.e. tracking of users' activities and movements in both the

643 http://www.facebook.com/press/info.php?statistics (as of January 10, 2012)
644 http://www.emarketer.com/PressRelease.aspx?R=1007386
645 http://www.gartner.com/it/page.jsp?id=1826814
646 Li/Chen 2010.
647 Krishnamurthy/Wills 2010.
648 http://www.gartner.com/it/page.jsp?id=1689814
649 It's a Social World: A Global Look at Social Networking. http://blog.comscore.com/

cyber and physical world, creates serious security and privacy concerns.[650,651,652,653,654,655] While most mOSNs require their members to share personal information as well as (an estimation of) their current location, users of such location-based services often lack an understanding of the privacy implications caused by the use of such services.[656] Some users are reluctant to reveal details about the online identity, or to agree to the collection and sharing of information about their presence or current location, at least not to the greater public. Others have additional concerns about the extent to which to trust the platform's operator to properly handle the information (personal data) they reveal and content (comments, photo) they generate on the platform. In addition to privacy issues identified for traditional OSNs, personal data along with information about the user's locations and online presence can be illegitimately collected and processed by various entities in the context of mOSNs.

A typical privacy threat in that context is the ability of third-party aggregators to track the users over time, generate a spatio-temporal correlation between location traces and a user's (pseudonymized) social networking identifier. From the information obtained, the third-party aggregator can then infer geographical points of interest, the exact home address, and even the real identity of a specific mobile user. Indeed, the traces and interest information can serve as quasi-identifiers that the third-party aggregators or advertisers may use to further profile, re-identify, and monetize users.[657,658] In a recent study, Wills et al. have studied privacy issues and problems that may occur in some of today's popular mOSNs.[659,660] The researchers examined popular OSNs such as Facebook, Flickr, and MySpace that have evolved to allow access from mobile devices, as well as the new mOSNs, such as Twitter, Foursquare, and Loopt, designed specifically to be accessed by mobile devices. They concluded in their report that most of the services leaked some kind of users' private information to at least three possible entities: i) actors within the mOSN (e.g. to friends of friends or the greater public); ii) users within other OSNs through dedicated API connection features, and; iii) finally to third-party aggregators and advertisers.[661] In many of those privacy leakage cases, the data disclosed contained the user's precise location, her unique networking identifier (device IP and/or social networking username). Based on this information and the details from cookies, third party sites can link the records they keep of users' browsing behaviours with profiles on OSN sites. Other work analysing potential risks of personal information leakage and further privacy design issues in mOSNs have been recently published in [662] and [663] respectively.

4.2.4 CLOUD COMPUTING

Cloud Computing refers to the long-awaited amalgam of computing power, software, storage and network capabilities, and other infrastructures made available as on-demand services over the Internet. As such, cloud computing is not only a new distributed computing paradigm, but also a new

650 Freudiger/Shokri/Hubaux 2011
651 Krishnamurthy/Wills 2010.
652 Griffiths 2010.
653 Krishnamurthy/Wills 2010.
654 Lardinois 2010.
655 Chen/Rahman 2008.
656 Friedland/Sommer 2010.
657 Freudiger/Shokri/Hubaux 2011.
658 Friedland/Sommer 2010.
659 Krishnamurthy/Wills 2010.
660 Griffiths 2010.
661 Krishnamurthy/Wills 2010.
662 Lardinois 2010.
663 Chen/Rahman 2008.

business paradigm. It enables flexible and dynamic IT service outsourcing with great efficiency, flexibility, scalability, and minimal operational overhead and financial cost. Activities previously done on private computers, and/or business functions and data once hosted and managed within the organization's boundaries, are now moving „into the cloud," as more individual users and organisations understand the cost-saving potential to elastic IT-related resources provided on-demand through internet technologies. Analysts have indicated that public and private organizations and individuals will embrace cloud computing models as a way to deploy software, store content, and manage resources.

As a new economic model for computing, Cloud computing has received a good deal of attention in recent years and is expected to see a massive global investment in the years to come. According to a report by Gartner, Inc., the Cloud computing industry is expected to show a strong growth through 2014, when the worldwide cloud services revenue is projected to reach $148.8 billion, from $68.3 billion in 2010 and $58.6 billion in 2009.[664]

Definition and Main Characteristics

Despite an increasing availability of products and services labelled as "cloud computing" technologies, the term itself is often used with a range of meanings and interpretations. Indeed, presently there is no consensus about what exactly cloud computing is.

The German Federal Office for Information Security (BSI) defines the term "cloud computing" as:[665]

> *" [...] the dynamic provisioning, use and invoicing of IT services, based on demand, via a network. These services are only made available and used via defined technical interfaces and protocols. The range of services provided under cloud computing covers the entire information technology spectrum and includes infrastructure (e.g. processing power, storage), platforms and software."*

This definition extends and provides a more nuanced view of a definition proposed by the U.S. Government's National Institute of Standards and Technology,[666] and used by the European Network and Information Security Agency (ENISA)[667] and other interest groups such as the Cloud Computing Use Cases group[668] or the Cloud Security Alliance (CSA)[669]

According to the NIST definition, cloud computing has three service delivery models and four deployment models. Note that other researches and groups including BSI, ENISA and the CSA have mentioned these models in very similar terms.

Service Delivery Models

Under the NIST definition, the three delivery models for cloud computing services are defined as follows:[670]

– *Software as a Service (SaaS)* SaaS refers to a model of service delivery whereby the consumer (i.e. individual end user, public, and private sector organizations) is provided access to a third party application on-demand, usually via the Internet. The application is thus configurable remotely. The cloud consumer does not own or manage the computational resources, platform and network infrastructure use to run it. Furthermore, the consumer neither owns nor manages the application itself. Typical examples of SaaS include applications for online collaborative text processing (e.g. Google Docs), contact data management and financial accounting (e.g. Salesforce CRM), etc.

664 Gartner 2010.
665 BSI 2011.
666 Grance/Jansen 2011.
667 ENISA 2009.
668 http://cloudusecases.org/
669 CSA 2009.
670 Grance/Jansen 2011.

- *Platform as a Service (PaaS)* here the service is an environment that is owned, delivered on-demand and managed remotely by the cloud provider. As an application framework, the computing environment (also called platform) provides the customer with standardised interfaces she can use to deploy and manage her own applications/services. However, she does not control the operating system, hardware or network infrastructure on which her own application is running, the provider does. Some well-known examples of PaaS are Microsoft Azure, Force and Google App engine.
- *Infrastructure as a Service (IaaS)* the IaaS model allows IT infrastructure resources such as processing power, storage, and network components or middleware to be delivered as on-demand services. This model allows customers to rent IT infrastructure (servers with certain processing, storage and network capabilities, and operating system of their own choice.) that are controllable via a service interface, and adds their own application/service on top. Accordantly, the can control the infrastructure and everything above it (i.e. the platforms and the software), but not the cloud infrastructure beneath it. Examples of IaaS include Amazon EC2 and S3, Terremark Enterprise Cloud, Windows Live Skydrive and Rackspace Cloud.

Each of these models allows cloud customers a ubiquitous access on a subscription or pay-per-use basis. Moreover, the on-demand functionality can be handled internally or by third-party cloud service providers, depending on the underlying deployment model.

Deployment Models

The NIST definition of cloud computing distinguishes four deployment models:

- *Public Cloud* The term public cloud refers to the deployment model in which infrastructure and computational resources that it comprises are made available to the greater public or a large group/organisation through the Internet. Public clouds are typically owned and operated by a cloud provider, which is by definition, not part, or different from any of the public cloud customers. The adjective "public" does not (always) mean that the cloud services provided are free or that customers data available in the cloud infrastructure are publically visible/accessible – users have to subscribe to access the services.
- *Private Cloud* In a private cloud, the cloud infrastructure is operated solely for a single organisation. The private cloud services may be managed by the organisation itself or by a third party. It may be located within the organization's domain (i.e. its own data centre) or in that of a different organization. In contrast to a public cloud, a private cloud has the potential to provide its customers with greater control over the infrastructure and the computational resources and data it comprises.
- *Community Cloud* A community cloud is one in which the infrastructure and computational resources are shared by a group of organizations that have common interests (e.g. the same need for particular data and applications). A community cloud can be operated by one of the group members or by a third party.
- *Hybrid Cloud* It refers to an integration of cloud deployment models. Here two or more cloud models (private, community, or public), each of which remain independent in itself, are interconnected and used via standardized or proprietary interfaces that allow Interoperability and Portability.

Benefits of Cloud Computing

Cloud Computing provides several benefits in contrast to traditional IT outsourcing and traditional hosting. The anticipated benefits of cloud computing can be broadly categorized into benefits for provider and benefits for consumers. Consumer benefits are those that an individual user and public and private sector organizations would be able to realize when using cloud computing services, while

provider benefits are those that a cloud service provider would be able to realize.

Benefits for cloud customers include:

- *Cost Reduction* Consumers/organizations are embracing cloud computing aiming at reducing their operation and management cost. By outsourcing computational, storage and networking needs, the company can focus on business-critical tasks, instead of dealing with the burden of running and managing non-essential hardware and software. Indeed, outsourcing or moving non-critical business processes to the cloud would free resources for the rest of the organization and help avoid additional costs (e.g. for new work force and training). Organizations can avoid expenditure on hardware and software; only using what they need. Entities from the public and private sector are already beginning to see the financial advantage of cloud computing. A few weeks ago, BBC reported that Banco Bilbao Vizcaya Argentaria (BBVA), the second-largest banking institution in Spain is switching its 110.000 staff to use Google's range of enterprise software.[671] The Arizona State University in the U. S. saves more than $500.000 per year using Google mail for its student e-mail service. Another example is the outsourcing of Rentokil Initial's email systems (incl. calendars, instant messaging, video communication, etc.) and its HR systems to Google's cloud, in 2009[672] and 2011[673] respectively.
- *Scalability (Elasticity according to the NIST definition)* Cloud computing allows organization (i.e. the consumer) to add and subtract capacity as needed. Thus, IT departments that anticipate variation in the organization service/resource can purchase as much or as little computing power, storage or networking resources as dictated. The result: the organisation pay for only what they use. For individual end users, cloud computing allows storage and management of more data than on private computers.
- *Flexibility* Cloud computing offers much more flexibility than past computing methods. Using the cloud computing services, organizations can obtain resources more flexibly, on an as-needed basis and then modernizing more swiftly once better technology is available. The update is highly automated. Thus, the organizations do not need to worry about keeping software up to date and are free to concentrate on core activities and business challenges. The service provisioning, automated in some cases, is adjusted to the customer's actual needs. Cloud computing allows organizations to roll out new services in record time, and for a fraction of the cost of maintaining an on-premise solution.
- *Enhanced mobility* Organization's employees and/or their customers can access information and services available in the cloud from anywhere at any time, from any computer, smartphone or tablet pc that is connected to the Internet.

Benefits for cloud providers include:

- *Resource pooling* The key benefit for the cloud provider comes from the fact that its resources are pooled to serve multiple consumers, typically via a multi-tenant model. The cloud service consumers usually do not know the exact location of the provided resources (e.g. where the outsourced data processing is taking place). The consumers may however, be able to contractually specify the location at a higher level of abstraction, e.g. the country.
- By enabling dynamic resource allocation (i.e. resources can be assigned and reassigned according to consumer demand), cloud computing is helping providers to offer services at attractive prices.

671 http://www.bbc.co.uk/news/business-16486796
672 http://www.computing.co.uk/ctg/analysis/1848259/why-rentokil-opted-google-apps
673 http://www.computing.co.uk/ctg/news/2125862/rentokil-initial-kills-premise-hr-systems

With the benefits and potentials of cloud computing in mind, technology leaders like Amazon, IBM, Microsoft, HP, and Intel have invested in the cloud computing vision and are now offering individuals, businesses, and governments a wide range of cloud-based products and services. Several analysts have recently predicted that the adoption of cloud computing among companies of all sizes will accelerate in 2012 and beyond. A 2011 survey on behalf of the telecommunications company Cable & Wireless Worldwide indicates that nearly half of multinational companies across the world have adopted cloud services (45% on average compared with 28% in 2010)[674]. As cloud consumers, the companies usually subscribe to applications running in the public cloud and make these apps accessible to both their employees and their customers. In this setting, there are different kinds of applications that are good candidates for moving to the cloud. According to the survey, the top cloud service companies are in the area of data management, including customer relationship management (CRM), document management, and business productivity applications e.g. email and IM applications. While a growing number of companies outsource at least some aspects of their enterprise content management and web conferencing to a cloud provider, only few are moving ERP (enterprise resource planning) functionalities into the cloud environment, the report says.

Beyond the application in enterprise domains, the benefits of cloud computing technologies have also been investigated in multiple other application domains. To name a few examples:

– Government Services and data in the Cloud Governments around the globe are increasingly adopting cloud-based solutions as means to eliminate redundant IT capacities and to standardize offerings across agencies, thus reducing costs and increasing efficiency (see e.g. the U.S. Federal Cloud Computing Strategy).[675] Prominent examples of national cloud initiatives recently announced are the US Cloud Storefront[676], the UK G-Cloud[677], and the Japanese Kasumigaseki[678] In each of these initiatives, existing government systems (e.g. for electronic procurement, payroll processing, accounting, and personnel management) and data are virtualized and hosted in the cloud, making them more accessible across government agencies and departments exclusively (private cloud) or to the greater public (public cloud).
– *Healthcare Cloud* Cloud computing concepts bring tremendous benefits to individuals/patients and healthcare organizations. In the context of the healthcare industry, cloud-based solutions enable individuals/patients to manage their personal health record (aggregation of information about the medical history of an individual) with more flexibility wherever they are. These solutions help health care providers and professionals (incl. insurers) organize, access, and share patient information and consequently reduce overall costs (e.g. by having lower IT personnel expenses), add flexibility, and improve efficiency with regard to the management of growing electronic medical records. Examples of healthcare cloud technologies are Microsoft Health Vault[679] (cloud-based personal health record application) and Dell's Unified Clinical Archiving[680] (cloud-based data retrieval and data sharing solution for the clinician).

674 Gillian Duncan (The National). Business forecast is cloudy. Aug 3, 2011. http://www.thenational.ae/thenationalconversation/industry-insights/the-life/business-forecast-is-cloudy
675 Kundra 2011
676 The US Cloud Storefront. Federal Cloud Computing Initiative, http://www.cloudbook.net/directories/gov-clouds/general-services-administration-gsa
677 The UK Government CIO Council, http://www.cloudbook.net/directories/gov-clouds/uk-government-cio-council
678 The Kasumigaseki Cloud, http://www.cloudbook.net/japancloud-gov.
679 http://www.microsoft.com/en-us/healthvault/
680 http://content.dell.com/us/en/healthcare/healthcare-medical-archiving-unified-clinical-archive

Privacy Concerns and Threats

Despite the tremendous benefits and promise of outsourcing data services to the commercial public cloud, cloud service users (organisations and individuals) often regard the issues related to trust in the security of the services provided and data protection as key barriers to a wider adoption of cloud computing. More precisely, cloud customers are very concerned about the risks and threats they are exposed to when outsourcing their services, processes, and data to commercial public clouds. Those risks and threats, which are amplified by the (on-demand) nature of cloud computing, include:

- *Loss of Governance / loss of control over data* By using cloud services, individuals and organizations typically surrender their ability to control and monitor the services there are using and data for which they are actually accountable. One consequence is that the cloud user is often not aware of the location (jurisdiction) in which its data is currently hosted and processed. In some cases, the data and processes outsourced in the cloud by the cloud client can be further outsourced to a subcontractor or supplier without client knowledge or explicit consent. Moreover, the loss of control over data by the client makes it almost impossible to reliably and completely delete/remove/erase personal or business sensitive data from the cloud after contract termination (i.e. after the client has left the service). It also makes it difficult for clients to check whether data is handled according to data protection policies they have negotiated with the provider.
- *(Compelled) Disclosure to foreign authorities/governments* Cloud customers' data is often stored and processed on machines located in different jurisdictions. Consequently, data may become subject to either relatively weak data protection laws or invasive legislations such as the U. S. PATRIOT Act[681]. Invasive legislations in particular are a source of concern for clients[682,683] since they may allow third parties (e.g. competitors) and government entities to sue the cloud provider and obtain a legal subpoena granting them access to customers' data stored in machines owned by that provider. Provisions in the U. S. Patriot Act even go a step further. They limit the cloud providers' ability to notify their customers that they received a court order / administrative subpoena. As a result, the customers may not even be aware of disclosure of their sensitive data by the provider. Possible damages from both subpoenas to cloud providers and the relatively weak data protection laws that providers and subcontractors may be subject to, are further consequences of the loss of governance by cloud customers.
- *Multi-tenancy and isolation failures* Virtualization of resources and resource isolation (e.g. via hypervisor or virtual machine monitor) are key technologies that enable the implementation of the concept of multi-tenancy, which in turn is fundamental to cloud computing. Relying on multi-tenancy, which allows a single resource to emulate multiple application instances, cloud providers can build infrastructures/platforms that are highly scalable and enable a single instance of a resource to be efficiently shared by different clients. The failure of resource virtualization and isolation mechanisms, e.g. due to the hacking of the hypervisor or virtual machines, can lead to unintended disclosure of sensitive data. Client's data may then become accessible to and manipulated by other tenants (competitors in the worst case scenario) with no requirement for disclosure.
- *Insecure Interfaces and APIs* Cloud customers typically rely on Web browsers and various plug-ins to access cloud computing services. To consume cloud services, an increasing number of those customers use browsers and other user interfaces (e.g. apps) that are embedded in mobile devices such as smart phones. On the

681 http://www.justice.gov/archive/ll/highlights.htm
682 http://www.cloudtweaks.com/2011/12/european-firm-refuses-to-go-on-the-microsoft-cloud-due-to-patriot-act-concerns/
683 http://www.wired.com/cloudline/2011/12/us-cloud/

other hand, cloud providers often expose APIs that their customers can use to manage cloud services or to build upon to create and offer new services. Both the vulnerabilities in client-side interfaces[684,685] and vulnerabilities in cloud provider's software stack can heighten risks regarding the theft of sensitive information (identity, credentials, company secrets, etc), the impersonation of trusted sources (e.g. the providers), the hijacking of individuals' account or service instances. Moreover, malicious entities may exploit these vulnerabilities to put cloud customers (and providers in certain cases) under active surveillance, and leverage the good reputation of their victims to launch additional attacks.

- *Provider-side misappropriation* Malicious insiders are great sources of threats in most organizations. In cloud computing environments, however, consequences of attacks by a malicious insider, e.g. the IT-system administrator of a cloud provider or subcontractor, can be far more damaging than in a traditional IT environment. In the context of cloud computing, security and privacy threats pose by inside attackers are amplified by the convergence of clients and their data under a single management domain, combined with a general lack of transparency into the policies, processes, practices, and hiring standards of cloud providers. Malicious insiders who have legitimate access to sensitive enterprises' / individuals' data can intentionally or accidentally make that information available to the wrong customers, competitors, foreign law enforcement authorities, or the greater public. Successful insider attacks against a cloud computing infrastructure could result in brand and financial damage (when enterprise confidential data are disclosed) or personal embarrassment (e.g. exposure of a patient's medical data to her employer or strangers).
- *Regulatory non-compliance risks* Companies that outsource their data processing to a cloud provider are often not sufficiently aware that they remain responsible for meeting regulatory requirements related to data protection.[686] They do not always know where their information resides due to the very nature of the cloud, which allows cloud clients' data to be shared and processed in different data centres located in different jurisdictions around the world. This can pose risks not only in terms of data protection and data security, but also with regard to the companies' responsibility to fulfil its regulatory compliance obligations. Indeed, moving to a public cloud may compromise years of efforts and investments in achieving certification (e.g. of the fact that the cloud client's internal controls and practices are specified and enforced in accordance with industry standards). This is particularly the case if the cloud provider is not able to:
  - provide evidence of its own compliance and /or the compliance of its individual clients with industry regulations such as PCI DSS for payment cards and HIPAA[687] for health data or with government regulations such as Sarbanes-Oxley[688] and the European Union Data Protection Act,[689]
  - allow the cloud client and auditor to assess its internal controls and practices (e.g. with regard to its commitment to store and process data only in specific jurisdictions).

The difficulty in fulfilling all compliance requirements is also due to the rapidly-changing standards landscape and possible inadequacy, incompatibility, or conflicts between the security policies and practices of the cloud provider and those of its consumers.

684 Marlinspike 2009.
685 Soghoian/Stamm 2010.
686 SAS-70. The Impact of Cloud Computing of SAS-70 Compliance Issues" www.clob.com ("Impact of Cloud Computing").
687 HIPAA 1996.
688 Sarbanes-Oxley 2002.
689 Directive 95/46/EC.

– *Vendor lock-in effect* A risk closely related to privacy and security concerns comes from the degree of dependence on the cloud service provider and the lack, or limited use of, open standards and interoperable IT technologies nowadays in the cloud. To put it simply, because standardised technology and interfaces are not widely adopted by cloud providers, customers may face issues such as provider lock-in and difficulties with data portability. That is, if, for instance, the provider declares bankruptcy or ceases to operate, its customers would have a hard time transferring their data back to their in-house IT system or migrating to another provider. Provider lock-in and data portability issues can therefore have serious consequences for the autonomy and personal choice of cloud customers, especially for that of individuals.

Further details and discussion on privacy and security concerns in cloud computing can be found in [690,691] and [692].

4.2.5 CYBER-PHYSICAL SYSTEMS

Technological advances in the fields of ubiquitous sensing, embedded computing, and wireless communication and networks are enabling the emergence of a new class of computing systems known as cyber-physical systems (CPS). CPS promise to bridge cyberspace, where information is created, exchanged, and transformed, and the physical world through networked embedded devices and sensors that enable real time information exchange between both worlds. It is viewed by many as the next computing revolution with potential for enormous societal impact and economic opportunities.[693,694]

CPS specify the seamless integration of and interaction between computation, communication, and control with the physical world.[695,696] Typically CPS invoke the integration of large scale and complex systems aiming at a pervasive and ubiquitous sensing, monitoring, and control of events in the surrounding physical environments. As a system of systems, a CPS consists of software-intensive systems and devices interconnected through heterogeneous communication networks, including Wireless Sensor Networks (WSN), Mobile Ad hoc Networks (MANET), and the Internet. Static/mobile sensors and networked embedded systems are key ingredients in CPS to facilitate interactions between human beings and their physical environments. Indeed, embedded systems and sensors with one or more multi-modal human-machine interfaces are used to seamlessly gather information from the physical world, make it available in the digital world for further processing, and to ensure that events in the physical processes affect computations and vice versa. These technologies also ensure that the integration of computing into individuals' physical environments take into account properties of physical processes such as time and space (cf. [697,698]).

The resulting convergence of heterogeneous communication networks with real-time systems, and distributed embedded sensor systems is not only enabling the dynamic mapping between computation and physical processes, but also the emergence of service-centric, adaptive, automated, and autonomous system environments. Such system environments typically consist of various computing, communication, and storage capacities and sub-systems that are tightly coupled with the physical world.

690 CSA 2010.
691 Grance/Jansen 2011.
692 ENISA 2009.
693 acatech 2011.
694 PCAST 2010.
695 Lee 2006.
696 Lee 2008.
697 Lee 2006.
698 Lee 2008.

CPS hold enormous potential for a wide range of (new) applications and technologies that span many industry sectors and affect many areas of life. CPS are forecasted to see explosive growth in the coming years and to become integrated into different areas of life. Cyber physical computing technologies include everything from relatively small everyday objects such as smartphones, smart home appliances, buildings, biomedical devices, and intelligent vehicles, to large systems such as smart cities, smart factories, and the national electrical power grid.

Today's application domains of CPS thus include areas as diverse as:

- Retail and wholesale trade (radio frequency identification (RFID) tags based monitoring of products' entire life cycle);
- Transportation Systems;
- Environmental monitoring and control;
- Critical public utility infrastructure monitoring (monitoring the structural health of bridges, dams, and remote management of the national electricity grid);
- Defense and aviation systems (battlefield networks and services) and;
- Telemedicine (implanted devices for remote patient health monitoring, early diagnosis, and treatment).

To illustrate the privacy and data protection issues/challenges in CPS, two representative application examples are discussed next: intelligent transportation systems and advanced electric power grids.

Intelligent Transportation Systems

Intelligent Transportation Systems (ITS) refer to the emerging new infrastructure platforms that aim at bringing significant improvement of efficiency, safety, and travellers' convenience in transportation systems of all kinds.

As application field for CPS, ITS envision a broad incorporation of embedded systems and wireless webs of sensors and actuators into elements of transportation systems, including vehicles, roads, bridges, train stations, airports, traffic lights, message signs, etc. Those networked embedded systems and sensors provide the computation and networking capabilities required to implement "smartness", and maximize the operational efficiency of transportation systems. For instance, transportation authorities and contractors may rely on a network of embedded systems and sensors to seamlessly gather any useful information about any elements of the transportation systems, (e.g. actual traffic conditions or the structural health of bridges) and other physical properties (e.g. weather condition or levels of air pollution). This information would then allow them to optimize both existing decision-making procedures and transportation services.

Such a convergence of transportation systems with Information and Communication Technology (ICT) promise the emergence of new products and services, many of which were barely imaginable just a few years ago.

ITS applications range from electronic toll collection / electronic tolling, to automatic early warning of nearby vehicles about road conditions (e.g. glazed frost roadway ahead), traffic statistics collection, and usage based vehicle insurance. As such, ITS applications rely on the sensing, processing and sharing of real-time information such as vehicles' current geographical locations and navigation directions; and information about traffic and weather conditions.

Even though the potential benefits for improving traffic safety and efficiency are conceptually appealing, privacy concerns exist therein, which if left unaddressed might prevent the large-scale adoption and use of ITS applications and ITS development. The fact that elements within transportation

systems, including vehicles, roads, bridges, train stations, airports, etc. are equipped with GPS, RFID tags, and other wireless communication devices may result in threats to the location privacy of specific individuals. ITS may enable malicious observers (law enforcement authority without warrant)[699] to track and monitor an individual's movements, activities, and communications over time, based on contextual information that vehicles' on-board communication devices and sensors reveal. This may occur without individual knowledge or consent. A closely related concern is the ITS ability to facilitate the collection and retention of more (personal) information than is absolutely necessary to fulfil the specified ITS purposes. As a result people interacting with ITS might have little control over what data from or about them are collected or how it will be used. Information about persons and their (current) environments that has been collected for one specific purpose may be abused for other, unauthorized purposes, i.e. to create individual profiles.

The integration of contextual information (e.g. current location, direction, movements, and physical properties) with other personal information (e.g. identity of users) could allow creating more detailed profiles. Such profiles may indicate, among other things, the locations a specific individual has visited, at what times, for how long, how often, her travel habits and driving pattern. While being of great importance when it comes to personalization of ITS service delivery, these profiles can also be used for unsolicitated location-based marketing; or to identify and discriminate against a certain segment of the population that has common characteristics.

Advanced Electric Power Grid[700]

The growing integration of ICT with national energy grids is currently shaping the overall vision of converging energy and information networks to a new infrastructure called Smart Grid. The latter describes enhancement strategies to address shortcomings of today's electrical grid with regard to the reliability and environmental sustainability of supply, the flexible and cost-effective control of transmission, distribution and consumption of electricity.[701,702]

According to the U.S. National Energy Technology Laboratory, the road map to accomplish the Smart Grid vision starts with the realization of two energy consumer-centric concepts: Smart Metering (SM) and Demand Side Management (DSM).[703] Both concepts describe a set of CPS technologies that allow the automatic collection of fine-grained data from metering devices located at customers' premises, and their transfer via wireless or wired channels to remote parties such as the Meter Data Management Agency (MDMA) or the Metering Service Provider (MSP).[704] Smart Metering (SM) and Demand Side Management (DSM) are designed mainly to intercept load information and provide both end customers and utilities with (real-time) feedback on power consumption patterns and levels. They also enable advanced control functionalities. That is, in order to balance or shift peak energy demand, SM and DSM technologies are used to remotely: disconnect several customers at the same time and in a controlled way; access and control home appliances (e.g. thermostats) in reaction to dynamic price signals or; perform operational tasks, e.g. remote management of field devices. As such, SM infrastructures and DSM systems, respectively, consist of smart meters interfacing with different components of the utility's ICT as well as with smart appliances in the home networking area.

Despite attractive features like low-cost management of the grid, load demand forecasting, and optimization of services (e.g. billing), the integration of modern ICT with electrical energy distribution infrastructures as incarnated by the

699 http://www.supremecourt.gov/opinions/11pdf/10-1259.pdf
700 Elements of this work have been previously published in Simo/Bayarou 2011.
701 NETL 2009.
702 NISTIR7628 2010.
703 NETL 2009.
704 IEEE Smart Grid Conceptual Model http://smartgrid.ieee.org/ieee-smart-grid/smart-grid-conceptual-model

Smart Grid vision may also raise serious threats with regards to customers' privacy and data security.[705,706,707,708,627] For instance, although energy usage data is needed by the utility and energy service providers, e.g. for operational and billing purposes, consumers' energy usage data collected by smart meters may also be used in ways which are potentially invasive of consumers' privacy. Privacy issues arising due to the accessibility and processing of such high-resolution information might range from:

- the unwarranted and/or inappropriate monitoring of activities within a home or an office;
- to unauthorized user profiling and tracking of PHV drivers' habits (leading to the disclosure of her location history), and;
- the unlawful access, use or modification of meter readings (e.g. for unsolicited services or fraud).[709,710,711,712]

Indeed, utilities and third party service providers[713] can potentially collect and retain huge amounts of customer-related data from which knowledge about their habits, activities and lifestyles can then be deduced.[714,715] The privacy issues surrounding such a collection and processing of customers' load information are obvious: details (about presence, activities, and appliances inside a home) can be detected by analysing the customer's energy data. These details could be reused for illegitimate monitoring or/and downstream purposes, e.g. the sharing with a third party without the customer's explicit consent or for abusive advertisements. Moreover, as consumption and generation load will be, in contrast to the situation in the current grid, automatically metered and exchanged through different networks and infrastructures that are partly deployed in hostile environments, the risk of eavesdropping, unauthorized access and disclosure, or fraudulent modification of meter readings (e.g. due to malware-infected firmware) emerges along with all the related legal and financial consequences (e.g. higher energy bills for the consumer).

Similar privacy concerns arise from other smart grid settings, e.g. the vehicle-to-grid paradigm. Here a specific combination of private information (e.g. the PHEV's current geographic position and its unique identifier) may be used to localize and track the "gridable" vehicle and its driver, at all times. This could allow creating additional individual's electricity usage profile and habits, this time outside their homes. From this information, it would then be easy to reconstruct her daily itinerary or identify sensitive places (e.g. drug treatment, abortion or AIDS clinic) she frequently visits.

Beyond the issues related to the pervasiveness of fine-grained monitoring of energy consumption, other privacy concerns emerge from the utility's foreseeable ability to enter its customers' private spheres, i.e. their homes. Depending on the setup and the underlying business model, third party service providers[716] may be interested in capturing the electricity demand profile of specific customers' "smart"

705 http://openenergymonitor.org/emon/sites/default/files/Energy%20indicators.pdf
706 Quinn 2009.
707 Thompson/Hall 2010.
708 Guarda/Zannone 2009.
709 NISTIR7628 2010.
710 Quinn 2009.
711 http://openenergymonitor.org/emon/sites/default/files/Energy%20indicators.pdf
712 Quinn 2009.
713 IEEE Smart Grid IEEE & Smart Grid. Smart Grid Conceptual Model -Service Provider http://smartgrid.ieee.org/ieee-smart-grid/smart-grid-conceptual-model#service-provider
714 Enev/Gupta/Kohno/Patel 2011.
715 http://www.daprim.de/?p=100
716 IEEE Smart Grid IEEE & Smart Grid. Smart Grid Conceptual Model -Service Provider http://smartgrid.ieee.org/ieee-smart-grid/smart-grid-conceptual-model#service-provider

appliances (by relying on advanced command and control functions) and monitoring whether these devices are operating at the highest level of efficiency, i.e. whether they are capable of delivering the expected results. Utilities might like to have the ability to remotely switch off any single customer's smart appliances when dealing with booming peak demands, even without customer's consent. They might want, in other contexts, to cut off energy supply, e.g. in case of non-paying customers or to isolate certain customers from the rest of the power infrastructure.[717] Note that this could be performed by terrorists targeting the national energy grid or intrusive government agencies interested in profiling and putting particular citizens under surveillance.

The customer-to-utility (two-way) interactions emphasize the privacy-sensitive nature of load information and other meter readings for both individuals and involved business entities. On the one hand, people may be interested in restricting the disclosure of the intimate details of their daily life or in keeping them absolutely secret. On the other hand, companies involved in a competitive energy market are interested in detailed customer data as enablers of highly personalized smart grid services. They want, at the same time, to prevent their rivals from gaining knowledge of their corporate business intelligence (e.g. due to intentional or unauthorised disclosure of intellectual property and trade secrets) when sharing energy-related information with them.

4.2.6 BIG DATA AND PRIVACY

The volume and variety of data generated and made accessible over the Internet has exploded over the last few years. Organizations and individuals use IT to carry out increasing amounts of their daily business interactions over the Internet. This has made it possible for users to generate and share a constantly growing quantity and variety of digital information online, and enabled organizations to routinely collect, manage and further transfer huge amounts of data (about customers) as part of their daily business operations. Such data can be replicated at low cost and is typically stored in searchable databases which are publicly (or at least easily) accessible. Indeed, the growth of ICT-mediated interactions between individuals and organizations is generating a tremendous amount of digital traces.

According to recent IBM estimates, 2.5 billion Gigabytes of data are created everyday around the globe, and the creation rate is growing continuously.[718] McKinsey estimates that the amount of digital content on the Internet is expected to grow by 44 times to 2020, at an annual growth rate of 40%.[719] This trend describes a phenomenon broadly known as the emergence of Big Data. The Big Data phenomenon itself is in part being enabled by the rising popularity of Web 2.0 (esp. online social networks) applications, the low cost of computation and storage, the rapid emergence of new computing paradigms such as cloud computing, breakthrough innovations in the field of data mining, combined with the wide availability of sensor-equipped and Internet-compatible mobile devices.

Nowadays, search engine providers are creating and maintaining ever-growing mountains of search logs that contain information which are an aggregation of what users of those search engines have had in mind at a certain point in time. Most online social network sites keep records of their users' social interactions, i.e. information the users, intentionally or accidentally, reveal when participating in such networking sites. Aggregating, storing, and analysing DNA-related data is becoming a key instrument for a growing number of companies that offer personalized healthcare services such as molecular diagnostics of diseases, DNA identification, and paternity testing. The explosion of mobile Internet and smart communication devices has given rise to a large

717 Anderson/Fuloria 2010.
718 http://www-01.ibm.com/software/data/bigdata/
719 Manyika/Chui/Brown/Bughin/Dobbs/Roxburgh/Byers 2011.

variety of context-aware or location-based services that not only help users to access online services from anywhere at any time, but also allow the sharing of user-generated contents with friends based on matching locations and interests. Such location-based services and technologies are facilitating data collection with greater granularity and frequency, and have thus given rise to large amount of geo-annotated content and transaction-related information circulating online. The success of (mobile) E-commerce features like personalization has lead to the collection of large volumes of sensitive information from customers, including their purchase history, product preferences, credit card numbers, home addresses, etc. Finally, as cloud computing gains popularity around the world and millions of individuals and businesses increasingly outsource storage and processing of sensitive business data to commercial public clouds, with the promise of minimal management cost, large volumes of data are pulled together, that can be aggregated and analysed for various purposes, including service delivery, auditing and compliance.

Although there is no commonly agreed upon definition of "Big data", the term is often used to describe the exponential growth and availability, as well as the complexity and speed of processing of various types of data that result from the interconnection of diverse data sources. Relying on advanced data analytic techniques, one may extract complex patterns, reveal correlations and cull valuable information from Big data. Examples of Big data sources include organizations' intranets, online government directories, large-scale sensor networks, clouds, search logs, websites, and web communities. Note that the flood of data and content contributing to the Big data phenomenon does not only include data originally created, stored and processed for a certain purpose, but also information which is a by-product of other electronic transactions. Furthermore, note that Big data is different from traditional data warehousing and types of business intelligence analysis that have been around for a while. Unlike the traditional procedure, a large part of Big data is unstructured and raw (a. k. a."grey data") data that is generated with greater velocity than ever before. Examples of such unstructured and raw data include email messages, text, images, audio and video files.

As data is increasingly viewed as a commodity and new form of currency, the emergence of such huge amounts of aggregated data and their linkability to other data sets clearly introduces a whole new set of opportunities and challenges.

Opportunities

The key opportunity is that Big data may significantly contribute to innovation and enable increased productivity and economic growth from which not only businesses but society at large would benefit.[720,721,722,723,724]

Making use of advanced data processing and data mining techniques, data analysts and other consumers of Big data (e.g. scientists, business and government entities) can compile and analyse large set of data to identify meaningful patterns of information. Indeed, relying on the mountains of data resulting from companies' internal processes and the growing torrent of heterogeneous data available externally, analysts may be able to get "formerly unanswerable questions answered"[725] and thus identify emerging trends early on. Companies could extract meaningful insights from data torrents to improve operational efficiencies, add intelligence to their processes, and thus gain competitive advantages.

720 Dacos 2012
721 Manyika/Chui/Brown/Bughin/Dobbs/Roxburgh/Byers 2011.
722 Bollier 2010.
723 IBM, On a smarter planet, answers are hidden in the data, Building a Smarter Planet: 2 in a Series, http://www.ibm.com/smarterplanet/global/files/us__en_us__intelligence__Data_visualization_4_6.pdf
724 Masiello/Whitten 2010.
725 Bollier 2010.

For instance, E-commerce platforms such as Amazon as well as retailers like WalMart are already able to leverage their large databases of consumer purchase histories, transactional information and inventory data to make item recommendations to potential customers, tailor their advertising strategies, or predict shifts in demand. McKinsey argues that an early adoption of the Big data phenomenon by (online) retailers would lead an increase of their operating margins by 60%.[726]

Search engine giants like Google use their ever-growing search logs not only to optimize users' online search experiences but also to better design their online targeted advertising models, and to identify and keep track of search patterns and trends. (cf. [727]) The ability to aggregate and analyse large sets of search queries allow Google, for instance, to predict and locate early signals of disease outbreaks (e.g. flu outbreaks)[728] with remarkable accuracy, in some cases much earlier than the healthcare authorities.[729]

A portion of financial institutions' routine tasks is to compile and analyse huge amount of personal, economic, and financial data, some of which are real-time streams (e.g. those from stock and financial markets), in order to calculate interest rates, or assess risks associated with possible new investments. Insurers can leverage big data techniques to retrospectively analyse years of transactional data to detect highly complex patterns, which they can in turn use for fraud detection, or to reduce their financial risks. Brokerage investment houses' ability to analyse huge sets of breaking news and weather information, gathered from the Web and other databases, in conjunction with market data, can allow them to tease out potentially valuable patterns that would otherwise remain hidden. They could then use those insights to predict stock market trends and improve trading decisions.

Entirely new business segments are emerging as consequence of Big data. For instance, healthcare data providers, who collect and analyse various types of data that are coming from different online and offline sources (e.g. from patients' body sensor networks, marketing surveys, electronic health records, government censuses) and are required to optimize healthcare services, would generate a market worth $10 billion by 2020, according to McKinsey.[730]

The energy sector (along with the emerging smart grid applications, see Section 4.2.5) is another field witnessing a growing use of data-driven processes and analytic data tools. The increasing deployment of smart meters, intelligent field devices, and other IT components within the energy infrastructure is generating a flood of new types of data. A near real-time collection and analysis allows utility companies to make sense of this data to improve the efficiency of power generation, transmission, and distribution, e.g. by being able to predict peak demand, to model and run higher fidelity simulations of power grids. Start-ups are developing applications based on behavioural analytics which enable end-users to understand, monitor, and actively control their energy usage. According to a recent study by Pike Research, the market for smart grid data analytics is expected to reach a total value of approximately $11.3 billion from 2011 through 2015.[731]

Big data is changing the public sector, too. Several governments have recently kick-started initiatives to transfer large government datasets, e.g. census data, traffic statistics, crime statistics, meteorological data, and healthcare data, to the Web. The move aims at promoting transparency and government accountability and achieving efficiency and effectiveness in government. Another hope is that the open accessibility and use of high value government datasets by private

726 Manyika/Chui/Brown/Bughin/Dobbs/Roxburgh/Byers 2011.
727 Google, Zeitgeist: Search patterns, trends, and surprises at http://www.google.com/press/zeitgeist.html
728 http://www.google.org/flutrends/
729 Carneiro/Mylonakis 2009.
730 Manyika/Chui/Brown/Bughin/Dobbs/Roxburgh/Byers 2011.
731 Pike Research 2011.

and commercial entities will drive innovations and create a new wave of economic growth. Examples of open-data government initiatives include the U.S. government website data.gov (whose purpose is to "increase public access to high value, machine readable datasets generated by the Executive Branch of the Federal Government")[732] and the UK Government site Data.gov.uk (a central repository for "non-personal data" acquired for official purposes)[733]. Many businesses and scientists view such freely accessible and searchable mountains of data as gold mines. According to the British government "[...] organizations, and even individuals, can exploit this data in ways which government could not be expected to foresee".[734] It estimates that public sector data in the UK is worth about £16 billion. The near future is expected to see an emergence of new commercial online services that leverage public sector data. For instance, types of online services will correlate publicly available property data (including prices and locations) with crime statistics, aiming at providing customers with recommendations about where, or where not, to buy a property. Start-ups would emerge that develop apps able to analyse mobile phone location signals in conjunction with governmentally-released crime statistics and up-to-date posts from online communities to indicate to users where "No-go-Areas" and "Safe Areas", respectively, are. For instance, Microsoft has recently been granted a patent for a technology that uses GPS signals in conjunction with the latest crime statistics, and weather data to calculate pedestrian routes. By plotting route predictions on a map available on GPS devices, the inventors at Microsoft claim their technology will help pedestrians to avoid an "[...] unsafe neighbourhood or being in an open area that is subject to harsh temperatures".[735] The use of advanced data storage, processing and analytical techniques to tap into the ever-growing masse of public sector data and to make relevant information available across different departments is also expected to help governments improve operational efficiency and reduce costs. According to McKinsey,[736] the European public sector is missing out on combined cost savings of around €100 billion per annum by failing to maximize the potential of Big data for operational efficiency.

The growing interest of law enforcement authorities and intelligence agencies in data from sources as varied as social communities, web search queries, mailing lists, financial records, travellers' biometric data, satellite imagery, and surveillance videos result in a flood of information. An aggregation and analysis of such data has the potential to yield useful patterns that in turn might serve to successfully investigate crimes, identify and track terrorists, detect tax fraud, etc. There is therefore a strong view among these authorities that the retention and mining of large amounts of telecommunications data is a key ingredient in resolving crimes committed by means of telecommunication networks or predicting the possibility of (cyber) attacks on critical infrastructure that are currently interfacing with Internet.

Challenges

While big data presents a number of new opportunities for individuals, organizations and society, it also introduces novel challenges related to such issues as data management,[737] security, trust and privacy.[738,612] The massive retention of

732 http://www.data.gov/about

733 http://data.gov.uk/about

734 The Government of the UK, Further Detail on Open Data Measures in the Autumn Statement 2011 http://www.cabinetoffice.gov.uk/sites/default/files/resources/Further_detail_on_Open_Data_measures_in_the_Autumn_Statement_2011.pdf

735 United States Patent 8,090,532 (Assignee: Microsoft Corporation (Redmond, WA)), January 3, 2012. http://patft.uspto.gov/netacgi/nph-Parser?Sect1=PTO1&Sect2=HITOFF&d=PALL&p=1&u=%2Fnetahtml%2FPTO%2Fsrchnum.htm&r=1&f=G&l=50&s1=8,090,532.PN.&OS=PN/8,090,532&RS=PN/8,090,532

736 Manyika/Chui/Brown/Bughin/Dobbs/Roxburgh/Byers 2011.

737 The huge quantity and complexity of formats of data becomes unwieldy and difficult for companies and governments to manage and understand. cf. http://www.gartner.com/it/page.jsp?id=1731916

738 boyd/Crawford 2011

individuals' behavioural, financial and other transactional data for analytic purposes may lead to the erosion of civil liberties due to loss of privacy and individual autonomy.

From a privacy and security perspective, the challenge is to ensure that individuals have sustainable control over their data, to prevent misappropriation and abuse by Big data holders, while preserving data utility, i.e. the value of Big data for knowledge / patterns discovery, innovation and economic growth. Main concerns about the privacy and security implications of Big data, result from the Big data holders' ability to collect, aggregate and analyse information from multiple otherwise isolated data sources. The following set of concerns and risks represent only a snapshot which may need to be revised and updated as Big data applications will continue to emerge:

- *The unauthorized access to and abuse of Big datasets* As more data is available and stored in databases accessible online, the risk of data breaches also increase. A recent series of high-profile data security incidents and scandals, e.g. Stratfor[739], Sony Corp.[740] and Wikileaks[741] have demonstrated that data breaches by those who have obtained access to sensitive datasets, legitimately or not, are devastating for both individuals and data holders.[742] For individuals, the consequence of such data breaches is the exposure of their identity attributes and other confidential information (e.g. credit card number) ether to an unauthorized party or to the greater public. For data holders, data breaches may result in brand damages (i.e. loss of customers' loyalty and partners' trust), loss of intellectual property, loss of market share, and legal penalties and fines in case of incompliance with privacy regulations.
- *Loss of control over datasets* When pulling data into applications and using it for all the purposes mentioned above, the concern/risk is that personal information torrents from external sources may come without users' informed consents. This raises questions regarding possible infringements of individuals' right to self-determination and Big data holders' ability to maintain regulatory compliance. Have individuals been given a genuine choice about their participation in Big Data-related processes? Do they always have control over whether or not their data is collected? Are they even aware of information from or about them being collected? Do they know how this information is being used? Indeed, information gathered from various sources may be reused for purposes and in contexts different from the ones, the data subject (i.e. the individual) had initially considered. In particular, re-purposing existing datasets to create completely new value also raise concerns about the need to re-seek informed consent for any secondary use of the data. From this concern emerges interesting questions: Who "owns" the data? Who should have access? For what purposes? In what contexts? With what constraints? Do data subjects know whether their personal information is being handled according to both their privacy expectations and the underlying data protection laws? Moreover, the growing ability to collect and analyse huge amounts of data, and the resulting deluge of digital personal data, make it hard to achieve a proper implementation of the notion of oblivion (a.k.a. the "right to be forgotten") in a Big data ecosystem.
- *Moving government data online poses (new) privacy risks* As said, the hope in most open data initiatives is that by accessing the wide range of high-value public sector data, businesses would be able to leverage it in ways which governments could not be expected to foresee. There is, for instance, an emerging personalized healthcare industry in which successful companies like Ancestry.com (http://www.ancestry.de/) and Navigenics (www.navigenics.com/) define their business models

739 Mills 2011.
740 Edwards/Riley 2011.
741 Rifkind 2010.
742 Nofer/Hinz/Muntermann/Roßnagel 2011.

around their ability to analyse genetic and genealogical information in conjunction with healthcare data coming increasingly from government sources.[743] However, the release of government records raises concerns about information privacy since they contain information spanning an individual's life from birth to death. Malicious commercial/governmental entities can re-use this information in a number of ways that may not be in line with existing data protection laws. With regard to the use of public records in the emerging personalized healthcare industry, there are growing concerns that open access to, and retention and analysis of naively "anonymized" DNA and personal medical data records could result in severe consequences not only for the individuals who have used those services, but also their relatives. "What happens when an insurance company gets a hold of these results and then denies your claims, or even insurance, because you have a possible genetic, pre-existing condition? You might not even have your DNA on file [...], but your sister, brother, mother, father, cousin, etc., might and their results could still tell a lot about you even though you've taken the precaution to not [to reveal your DNA]".[744] Other privacy concerns raised by the move to make government data widely available online include gleaning insights from a single or a combination of records (e.g. public health registries, tax, and custody records) and then abusing it. The information extracted could then be linked back to specific individuals, abused by identity thieves or misused to threaten the safety and damage the reputation of certain individuals.[745]

– *Big data can dramatically amplify the privacy implications of database correlation* When integrating information from diverse data sources, e.g. web communities, government online directories, and modern enterprise customer relationship management (CRM) systems, it is possible to combine and match single pieces of data across boundaries. Some of these pieces of information alone might be non-identifying and data holders may therefore tend to consider them as not covered by existing data protection laws. But adversaries (e.g. Big data analysts) with access to ever-growing storage and processing capabilities and advanced data mining tools can perform the combination and, intentionally or accidentally, identify new inferences or create new sets of personal information that can then be used to cause substantial damages or distress in various other contexts. Note that privacy issues as unexpected consequences of correlating pieces of public data are not new.[746,747,748,749] Several years ago, Latanya Sweeney showed that it is possible to retrieve personal health data by cross-linking an allegedly anonymous database of state employee health insurance claims with a publicly available voter registration database.[750] More recently, Acquisti and Gross have demonstrated that one can predict an individual's social security number with remarkable accuracy using only public data.[751] For their tests, the scientists used the publicly available U.S. *Social Security Administration's Death Master File*[752] and other personal data from multiple sources, such as data brokers or profiles on social networking sites. From this perspective, Big data could make things worse. Indeed,

743 In the UK, this may contain DNA records of suspects who were arrested but subsequently acquitted or never charged, http://www.telegraph.co.uk/news/uknews/law-and-order/8660821/Innocent-peoples-DNA-profiles-wont-be-deleted-after-all-minister-admits.html
744 http://www.lossofprivacy.com/index.php/2007/06/ancestrycom-adding-dna-test-results-to-their-site/
745 Bermann 2006.
746 Winkler 2006.
747 Acquisti/Gross/Stutzman 2011.
748 Acquisti/Gross 2009.
749 Sweeney 2002.
750 Sweeney 2002.
751 Acquisti/Gross 2009.
752 http://www.ntis.gov/products/ssa-dmf.aspx

the rise of large pools of databases that interact with each other, combined with the emergence of powerful new data analysis tools, clearly increase the potential for privacy violations resulting from dataset correlations. Examples of such violations include user profiling and re-identification, identity theft, exclusion and discrimination against individuals or minorities.

– *The ease with which an unfair discrimination directed at certain individuals might occur.* While the growing ability to collect and analyse vast amounts of data may reveal high value insights used to improve decision making, operational efficiency, and services delivery, it also allows the discovery of information that might be used for negative discrimination. Insurance companies and healthcare providers able to collect and analyse information from public health repositories, poorly de-identified patient databases, disease-related web search logs, or patients' online communities, can capture insights, which they can use to optimize the quality and efficiency of their services. Other industries (e.g. hotels) use similar approaches to collect and analyse vast amounts of information about available seats or rooms, marginal costs, and expected demand. Based on the findings that the advanced analysis revealed, the companies can vary their prices profitably. However, individuals and privacy experts regard such practices as potential sources of privacy violations and unfair discriminations. For instance, insurers can use Big data techniques to profile, reverse identify, and then discriminate against individuals with pre-existing conditions or those with certain health risks (e.g. by denying healthcare coverage or demanding higher fees). In a recent article, the New York Times reported on how specialized software is allowing real estate firms to automatically calculate and suggest the highest possible rent price to charge for a particular apartment by analysing mountains of information including real estate supply and demand statistics, dynamic market prices, marketing surveys, and government censuses.[753] Some have expressed concerns that this practice may lead to an increase in housing discrimination, i.e. it would make it difficult for certain classes of citizens (e.g. renters) to find "affordable" rental housing. In addition, combining data about properties and government-released crime statistics and plotting them on a map may lead to discrimination against certain neighbourhoods (bad reputation) and thus negatively affect the property values in that area. Another closely related concern is about the ethical collection and use of Big data. As it has been colloquially put by boyd and Crawford: "Just because it is accessible doesn't make it ethical".[754]

These concerns threaten to undermine the potentially highly beneficial opportunities of Big Data.

4.3 PRIVACY-THREATENING TECHNIQUES ON THE WEB

We reviewed some of the most common (potential) privacy-invasive applications on the Internet. In order to examine the privacy risks from a technical point of view we need to review the techniques that collect information on individual web users. That is, techniques which track the web activities of individual web users; such techniques can be categorized as tracking techniques. In addition, we need to study techniques that process the raw data in order to relate data from different sources to one individual user, gather relevant information on individuals, and eventually deduce and predict information from the raw data. Such techniques can be categorized as profiling techniques. Acquiring information on web users, tracking their web activities, and processing such information is not necessarily by nature an invasion of privacy; but it provides the foundation for privacy violations. Gaining information about web users is not a recent matter, in fact, it has been practiced for at least a decade.

753 http://www.nytimes.com/2011/11/30/realestate/commercial/landlords-use-computers-to-arrive-at-the-right-rental-fee.html
754 boyd/Crawford 2011.

The economy is using targeted web advertising progressively; so-called Online Behavioral Advertising (OBA). Therefore, tracking and data collecting techniques to identify the user's interests and preferences are progressing more than ever. The emergence and development of various platforms such as e-commerce platforms and Online Social Networks (OSN), on which the user intentionally submits personal data, has made the situation more acute. Furthermore, data processing techniques which can extract additional information from user's personal data from large databases have been advancing vastly. In such an environment it is of great importance to investigate the privacy risks for individual web users and privacy threatening techniques on the web. We are going to investigate such privacy-threatening techniques; which are the technologies that are focused on acquiring information that an individual may wish to keep private. We examine privacy-threatening techniques in three groups: tracking technologies which acquire information on individual web users; profiling techniques to accumulate and classify the raw data; and issues related to the security of long term storage of data.

We proceed as follows. The next section, Section 4.3.1, reviews the common technologies for tracking the web activities of individual users; including the most common web identifiers. Section 4.3.2 presents techniques that are used for user profiling, namely data collection and data processing techniques. Section 4.3.3 analyses the consequences of long term storage of data from the privacy perspective.

4.3.1 TRACKING WEB USERS

In this section, we investigate the most common techniques to track the activities of web users. Tracking techniques follow the web activities of individual users, i.e. browsing activities of an individual user. To distinguish the web activity of a user from web activities of other users, the user has to be identified. Hence, user tracking practices require the identification of a client machine.[755] As a consequence, identification methods, such as cookies, can also be used for tracking. To identify a web user, the user either has to explicitly provide some kind of identification, for example by logging into her Facebook account, or some identifiers have to be set implicitly on his browser or machine without any user interaction. We review first the most common implicit identifiers and proceed then with the main tracking techniques on the web.

IP Addresses

Internet Protocol (IP) address is a label assigned to each device that is connected via the Internet Protocol[756]. IP addresses are the most common user identifiers on the web. They are used for all interactions between the user's machine and the web, i.e. web search engines (discussed in 4.2.1), web browsing, and e-commerce application. Currently, the two latest versions of IP addresses, namely, IP V4[757] addresses and IPV6[758] addresses are both used on the Internet. IPV4 addresses consist of 32 digits and IPV6 of 128 digits. From IP addresses, information such as the host or network and the location from which the device is connected can be identified. However, IP addresses cannot always be considered a reliable identifier. For example, a user might be assigned to an almost arbitrary and temporary IP address[759]; or different users may use the same IP address such as two family members that are using the same internet connection.[760]

Cookies

In this section cookies and their role as identifiers for user tracking are explained. The underlying protocol for data

755 Schmücker 2011.
756 Described in the Internet standard document RFC760.
757 Described in the Internet standard document RFC 791.
758 IPv6 was developed by the Internet Engineering Task Force (IETF) and is described in Internet standard document RFC 2460.
759 Kristol 2001.
760 Kristol 2001.

communication on the web is HTTP (HyperText Transfer Protocol). HTTP operates on a request-response basis and is by design a *stateless* protocol. Hence, HTTP requests are treated independently from each other. The IP address of the sender of an HTTP request is submitted, however, we have seen that IP addresses cannot serve as a reliable identifier. Therefore, two HTTP requests which have been sent by the same user could not be correlated. In order to keep track of the sender of an HTTP request in a browser-server communication, cookies have been introduced as an addition to HTTP.[761,762,763] A cookie is a text-only string that is entered into the browser's memory; the server and client pass the cookie back and forth during their interactions in order to keep track of the state of their interactions.[764] The use of cookies can have several objectives such as[765]: to identify and authenticate the users[766]; to store the user's preferences and settings such as language preferences; to maintain a web session; to create user profiles and track the user, and for targeted advertising.[767] For example, web applications such as OSN (discussed in 4.2.3) and E-commerce applications (discussed in 4.2.2, online targeted advertising) use cookies in order to identify (and eventually track) individual users. In the following, we describe in detail how cookies are initiated and used in HTTP communications. Each HTTP request consists of a header; the header of a request contains control information and transfer information for HTTP (e.g. destination address).[768] When a browser (client) for the first time loads a web page from a web server, the client sends an HTTP request to the web server. The server includes a cookie in the header of the response. This cookie will be communicated between the web server and the browser for all their future interactions until the expiry date[769] of the cookie. The main attribute of a cookie is a name-value pair; in which the value is the text string which serves as the identifier. The name is used to recognize the cookie and the value is the identifier (representing the user or her browser). The value can refer to a preference of the user or only serve as an identifier such as numbers or alphabetic letters. Figure 1 shows a cookie which was set on the Firefox browser with the name "*GoogleAccount Locale_session*" and the value (content) "*de*" which indicates the country (in this case Germany) from which the user is connected. A cookie can also have other attributes that are used for controlling purposes; such as a path and expiration time or maximum age. Only the name-value pair is mandatory. Cookies can also be designed to store the user's browsing history, making her a data collection mean[770]; which we discuss in the next section. Since most of the browsers follow the same origin policy,[771] which allows only servers that initiated a cookie to access it, generally, the browser sends only the cookie's name-value pair to the server. Cookies are usually only sent to the server which has initiated the cookie to the browser. However, a web page may contain context from other servers (called third party server such as advertising companies, subcontractors, etc.). For example, when a Yahoo website[772] is loaded, the advertisements that are displayed on the Yahoo website are loaded from third party servers. Since, in order to load the website, HTTP requests are also sent to such third party servers; they may also set cookies (called third party cookies) on the client browser without the awareness of the user.

761 McKinley 2008.
762 Tirtea/Castelluccia/Ikonomou 2011.
763 Kristol 2001.
764 Whalen 2002.
765 Tirtea/Castelluccia/Ikonomou 2011.
766 Instead of explicitly logging in with username and password.
767 Based on the user's interests acquired by monitoring his most frequently visited sites.
768 Kristol 2001.
769 The expiry date depends on the use of the cookie; cookies that are set for maintaining a web session expire when the web page or browser is closed. On the other hand, cookies that are set for authenticating have a longer lifetime.
770 Stackoverflow 2010.
771 W3C 2010.
772 Yahoo counts as the first party server.

Beside the original HTTP cookie described above, there are more persistent cookies that are used for tracking users, so-called Supercookies such as Flash cookies and Evercookies. These kinds of cookies are harder to erase and in some cases have regenerating abilities.

Adobe Flash Local Shared Objects (Flash cookies)

Adobe Flash Local Shared Object is information stored on a user's computer to facilitate Adobe Flash applications,[773] i.e. user preferences. In addition, the local shared objects have the same functionality as HTTP cookies, containing attributes for unique identifiers and are therefore called Flash cookies. Flash cookies are stored outside the browser's memory. Therefore, the browser has little control over the Flash cookie.[774] Hence, by deleting the cookies on the browser's setting, the Flash cookies are not affected.[775] In addition, since Flash cookies are not stored in the browser's memory, they can identify the user even if she is connected from a different browser; for example, the Flash cookie was set on the user's system when she was connected with a Firefox browser, after closing Firefox and connecting to the web with a Google Chrome browser the user is still identifiable.[776] In contrast to HTTP cookies, which either last only till the end of a web session[777] (session cookie) or have an explicit expiring date (persisting cookie), Flash cookies have, by default, no time limit. Having no expiration date enables web sites to use Flash cookies to automatically re-spawn (regenerate) HTTP cookies if they are deleted, like a hidden backup.[778,779] Any websites that use Adobe Flash can store a Flash cookie on a user's computer.

HTTP cookies and flash cookies can also be programmed to store a user's recent browsing history.[780] Flash cookies can store up to 100KB while normally HTTP cookies only up to 4 KB, which makes them more suitable for storing the browsing history of the user.

Evercookies

An Evercookie is cookie data which is set on a browser, designed to be resistant to elimination. Evercookies are stored with several types of storage mechanisms that are available on the local browser.[781] In addition, the Evercookie regenerates itself as soon as the user deletes the cookie. Evercookies are not yet used in practice; they are rather designed to invoke the possibility of everlasting cookies.

Browser and OS Fingerprints

Another technique to identify a web user is by producing a device fingerprint [782] of the user's browser. Based on the browser configuration such as fonts, screen resolution, language, etc., a browser can be identified within 20000 other browsers.[783,784] A fingerprinting algorithm computes the browser fingerprint which is used to identify the browser.[785] Moreover, to identify a web user, Operating System (OS) fingerprints can also serve as identifiers. OS fingerprints are computed by a fingerprinting algorithm based on the

773 "Flash is used extensively for advertising thanks to its support for animations, multimedia, and its flexible scripting language," Primelife 2011.
774 Although recently some versions of Firefox, Chrome and Safari in cooperation with Adobe Inc., improved their privacy mode functionality by increasing the control of the browser on Flash cookies.
775 Soltani/Canty/Mayo/Thomas/Hoofnagle 2009.
776 In case of a HTTP cookie, if the user is connected through a different browser, she is not identifiable anymore.
777 A web session is a series of interactions between the server and the client during the span of a single connection.
778 Singel 2009.
779 Soltani/Canty/Mayo/Thomas/Hoofnagle 2009.
780 Stackoverflow 2010.
781 Kamkar 2010.
782 A (device) fingerprint is a unique summary that is computed from a software or hardware settings, and can uniquely distinguish the (device) software or hardware.
783 Eckersley 2010.
784 Castellucia/Druschel/Fischer Hübner/Pasic/Preneel/Tschofenig 2010.
785 Eckersley 2010.

attributes of the user's operating system.[786] OS and browser fingerprints can ideally be used alongside other identifiers such as IP addresses or cookies. In addition, in the case of browser fingerprinting and OS fingerprinting, data on the browser or the operating system is collected, such as user preferences and setting

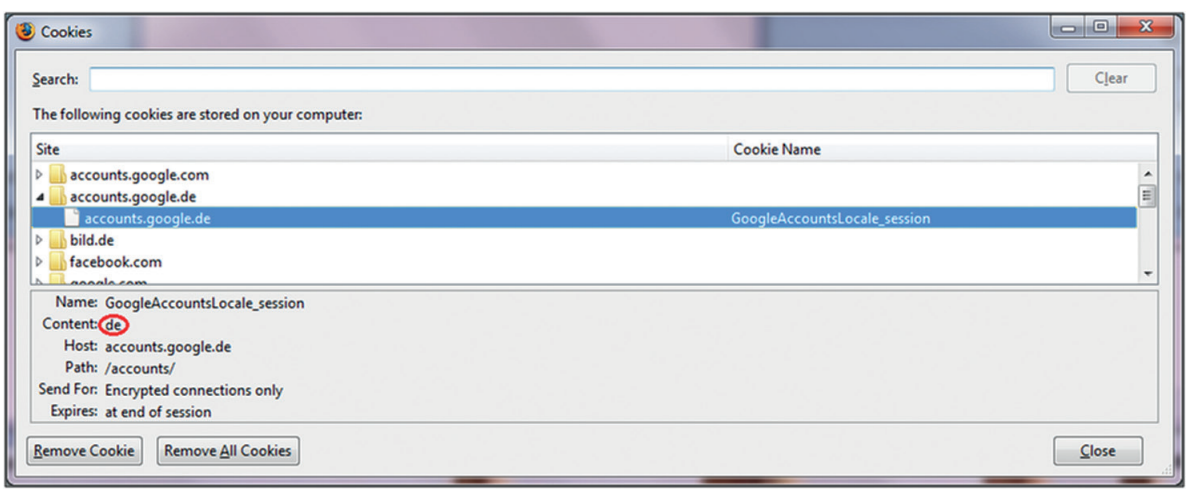
Web Bugs

In this section we describe web bugs; which are used for tracking the user's clickstream across multiple web sites. Web bugs (also called web beacons) are used to inform the web bug creator when an email is opened or web page is visited. Web bugs are small images (usually transparent, 1 * 1 pixel) embedded in a web page.[787,788] The image is handled like any external image in a web page; external images (also ads, videos, etc.) are requested from the source web server. When a web page or email (uploaded from a so-called first party server) contains a web bug, the browser sends an HTTP request to the web bug source server (third party server) in order to retrieve the image. Web bugs do not store or save data of the user. They simply require the user's device, without the user noticing, to send an HTTP request to the web bug creator every time the user visits the web page that contains the web bug. Therefore, the third party server is informed that the web page was viewed by the user's browser. Advertising companies place web bugs on several web pages, therefore their web server can track the user's clickstream across those web sites.[789] Advertising companies use web bugs commonly to track the user's browsing history in order to learn about her interests for targeted advertising.

Page Tagging or JavaScript Tags

A JavaScript tag is a JavaScript code which is embedded into a webpage. When the web page is loading, the JavaScript code is downloaded and then executed. Page tags are an

Figure 1: A cookie set on the Firefox browser which has stored the country from which the user is connected.



786 Trowbridge 2003.
787 Steindel 2011.
788 Dobias 2011.
789 Castelluccia 2012.

extension of the idea of web bugs. The JavaScript code can be programmed to send user data to the data collection server, e.g. Google Analytics.[790,791] Page tags can be used to collect and send the history of visited links (so-called history sniffing),[792,793] click data, page view, and cookies. They also can be programmed to update cookies.[794] JavaScript tags are currently one of the most common data collection methods on the web; due to their flexibility in defining the kind of data that has to be collected.

4.3.2 USER PROFILING

In this section we investigate user profiling practices. User profiling refers to collecting and processing data from the web that is associated with a specific user. The data is collected with different collection techniques, which also include information that is retrieved by user tracking (explained in 4.3.1) such as the browsing history of an individual user. The collected data, which may be collected from different domains (e.g. various OSNs, or E-commerce applications), is then processed, e.g. combined and cross-referenced, in order to associate relevant data with a specific user. In the next section we review the most common data collection techniques on the web. Subsequently, Section 4.3.2.2 investigates the information processing practices that are applied to raw data to deduce new knowledge.

4.3.2.1 Data Collection

This section investigates some of the most important techniques and practices for data collection, excluding user-tracking techniques, explained in 4.3.1, which often can include data collection techniques, e.g. page tagging.

Data collection practices fall into two main categories, *explicit data collection and implicit data collection*.[795] However, a combination of both of them is frequently used in practice. In explicit data collection, the user submits information about herself intentionally, e.g. she explicitly provides the information to a platform such as posting a photo on an OSN. In implicit data collection the data is accumulated without the user's participation and sometimes without the user's consent. The user does not always have knowledge of the fact that data about her is being collected. It is obvious that explicit data collection and information sharing and dissemination are privacy-threatening practices. Therefore, we review in this section the implicit data collection techniques. Data collection techniques can be categorized into two main categories; *server-side data collection and client-side data collection*.[796] In client-side data collection the data collection is applied on the client side. Tracking techniques explained in 4.3.1 such as web bugs and page tagging are client-side data collection methods. In server-side data collection techniques, the data is accumulated at the hosting server. Browsing activities and search interactions are aggregated by server-side data collection techniques. In this section we first review the most common server-side data collection methods and then discuss *history sniffing and monitoring software* which are client-side data collection methods.

Log File Generation

Server log files are generated for several purposes such as error capturing (error handling), by law enforcement. Such log files can be also used to generate statistics and for user profiling. Server log files include, among others,[797] web log files that store browsing activity (clickstream data)[798] and

790 Schmücker 2011.
791 Kaushik 2007.
792 Weinberg/Chen/Jayaraman/Jackson 2011.
793 Jang/Jhala/Lerner/Shacham 2010.
794 http://www.ehow.com/how_8219518_update-cookies-via-javascript.html.
795 Cranor 2003.
796 Clifton 2008.
797 Log files of Internet Service Provider (ISP), Proxy server log files, etc.
798 Clickstream data of a user is a sequence of the visited web pages by that user.

search log files that store search queries of the user.[799] A web log file is a text file in which the HTTP requests to the server are stored.[800] For example, when a user's browser loads a web page, the HTTP request to the web server (pages, images, PDFs, videos, etc.) are logged in web log files. The structure of the log file depends on the server which is generating the log file.

The information that is stored in a web log file contains, among other things[801], the sender's IP address, the time at which the request was sent (time web page was visited), requested URL of the web page,[802] and the cookie.[803]

A search log file is a text file in which search queries,[804] are stored, that are submitted during a search. The privacy issues of logging by the search engine have been discussed in Section 4.2.1. The search log files include also connectivity information such as IP address and the browser version of the user who has submitted the search query.[805] Web or search log files can then be analysed by log file parsers in order to extract the desired information about an individual user. Since the log files are generated on all web activities, log file generation and analysis is one of the most common server-side data collection practices.

Deep Packet Inspection

The data moves in the internet in form of packets, each consisting of a header (containing transfer information) and a payload (containing the actual information that is sent such as the content of an email). Inspecting these packets is called packet inspection or packet sniffing[806] which is often used to validate the network traffic by the network or system administrator.[807] A typical packet sniffer, performing Shallow (or Stateful) Packet Inspection (SPI), captures the data on the packet header of the inspected packet including information such as the destination of the packet.[808,809] A more (privacy) invasive packet inspection is Deep Packet Inspection (DPI).[810,811] DPI is also used legitimately to monitor the network traffic in order to analyse network problems.[812] However, the captured and analysed data may be used also for data collection purposes about web users[813] and therefore DPI can be also considered a privacy invasive technique.[814,815] DPI inspects and analyses not only the header of the packets, but also the payload of the packet. DPI can be compared to reading a post card or "postal employees opening envelopes and reading the letters inside."[816] The header of the packet can be compared to the address field in the post card; the payload of the packet to the message on

799 Kaushik 2010.
800 Since, all web requests of a user go through the ISPs; therefore, ISP servers are a suitable source of log file data on a user's activity.
801 Information that was provided by the header of the HTTP request such as Host, RFC931, Username, Timestamp, Request , Statuscode, Byte, Referrer, Useragent, and cookies.
802 (via referrer header).
803 In addition, a typical HTTP request header contains information such as the current and previous URL (via referrer header), email address, language preference, and etc. (Castellucia/Druschel/Fischer Hübner/Pasic/Preneel/Tschofenig 2010, P.5).
804 "along with basic connectivity information such as IP address and browser version" , Kaushik 2010.
805 Kaushik 2010.
806 Ansari/ Rajeev/ Chandrashekar 2002/2003
807 Bradly 2012.
808 *Id.*
809 Stateful packet inspection is also used by security mechanisms such as Firewalls.
810 Mochalski/Schulze 2009.
811 AbuHmed/Mohaisen/Nyang 2008.
812 Daly 2010.
813 Tene/ Polonetsky 2012.
814 http://epic.org/privacy/dpi/
815 Del Sesto/Frankel 2008.
816 The Privacy Implications of Deep Packet Inspection: Hearing Before the Subcomm. on Commc'ns, Tech., & the Internet of the H. Comm. on Energy & Commerce, 111th Cong., 2009. (statement of Leslie Harris, President & CEO, Ctr. for Democracy & Tech)

the post card. However, since the reader does not usually understand the format and language of the payload it can rather only scan and search for patterns which can be compare to reading a postcard that is written in another language and the reader is looking for words which he knows by sight.[817]

History Sniffing

History sniffing is a client-side data collection method. History sniffing is applied in various forms; we present two classic examples of history sniffing attacks: the CSS visited link attack and the Cache Timer attack.

When a user visits a website the browser remembers this visit. Thereafter, hyperlinks of the visited web sites, by default, are colored differently from those the user hasn't visited (unvisited sites in blue and visited sites in purple).[818] JavaScript scripts can inspect such markings in order to find out which websites a user has visited.[819]

Another history sniffing attack is the Cache Timer Attack.[820] Each time a user visits a web site the browser stores a local copy of the files on a cache[821] memory. For the next visit to the website the stored files are loaded directly from the cache instead of loading them from the corresponding web server.[822] By monitoring how long loading a website takes for a browser it can be found out whether the web site was visited before.[823]

Monitoring Software

Monitoring software are client-side data collecting techniques such as *Trojan horses*, browser extensions, browser toolbars, software agents. Monitoring software can be designed by a government, software companies, and even individuals. It is common that the user installs the monitoring software himself, unaware of the data collection functionality of the software. In this section we review few examples of monitoring software. Trojan horses are software that have a secondary function other than their claimed functionality. For example, a video player may be a Trojan horse. After the user has installed the Trojan horse (the video player), it can, in addition to the expected function, gather information and send it to a server. *Browser extensions* are additional software which are installed on the browser in order to extend the browser's functionality and add a specific ability to the browser. Such extensions are also often designed by third parties. For example, the Firefox browser allows plugins to be installed to use Google Talk or view PDF files. Examples on browser extensions that gather user's data are Google Reader Notifier[824] for Firefox and Google Plus extension for Chrome.[825] *Browser toolbars* are graphical user interface components on which buttons, menus, and icons are placed in order to simplify the access to functions and components of the browser. However, they can also be used to collect data from the user's web activities such as the visited web pages or the search terms utilised by the user.[826] *Software agents* are software that act on behalf of an organization or another user.[827] However, they can be

817 Mochalski/Schulze 2009.
818 Coloring the visited links is achieved through CSS (Cascading Style Sheets; defining the appearance and formatting) working with the user's web browser, Albanesius 2012.
819 Landesman 2012.
820 Albanesius 2012.
821 Cache memory is a small, high-speed buffer memory used to hold temporarily the contents of the main memory that are currently in use. Smith 1982.
822 to speed up the performance.
823 Landesman 2012.
824 Google Reader 2012.
825 Cubrilovic 2011.
826 Kaushik 2010.
827 Software agents are used in various domains, mainly monitoring traffic network and surveillance for network errors.

used to collect user data and forward it to a remote server. In contrast to the previous monitoring software examples, software agents are not installed by the users, rather by network administrators.

4.3.2.2 Information Processing

The collected data often turns out to be less useful if no processing is applied to the raw data. Therefore, information processing practices are used to extract, gain, and deduce useful information out of unprocessed data. Processing raw data has several purposes such as identifying individuals or groups out of anonymized databases[828] (de-anonymizing), accumulating and summarizing the data (data aggregation), and extracting unknown information from the raw data (data mining). In the next section, such processing practices are discussed. In particular, we review data aggregation, data mining, and de-anonymization which are, to our belief, the main privacy-invasive data processing practices, although not the only ones.

Data Aggregation

Data aggregation refers to the collection, storage, accumulation, and combination of raw data. Data which is collected from different domains/sources is combined, bound, and associated with other data by data aggregation. For example, data that is collected from a user's various OSN profiles,[829] such as Facebook and LinkedIn;[830] or her data from her Facebook profile is combined with her browsing activity history. Therefore, data aggregation provides a much more comprehensive view of the user's profile than the data that is collected only from one domain/source.[831] The aggregated data then can then be used for other data processing techniques such as data mining or de-anonymization. Hence, both data mining and de-anonymization usually include data aggregation as their first phase of procedure. Centralized databases which contain massive quantities of aggregated data, that are organized and referenced in a fashion that facilities the later retrieval of the data, are called data warehouses. Pure data collection or gathering is also called data warehousing.[832]

Data Mining

Data mining refers to discovering relevant and potentially useful information or knowledge from large amounts of data, which was unknown before.[833] Data mining techniques which are applied to web documents are called web mining. Web mining practices can be classified into three main domains: web usage mining, web structure mining, and web content mining.[834,835] Web usage mining, also called web log mining, studies the user's navigational behavior based on access log files, among other sources.[836,837] Therefore, web usage mining is causing potential privacy risks for web users.[838] The data sources for web usage mining include clickstream data, access logs, referrer logs, agent logs, client-side cookies,[839] and web activity history (i.e. purchase history). In addition to the

828 An anonymized database is a database in which the attributes which identify individual user s are removed, so that a data cannot be linked to a specific person.
829 Irani/Webb/Pu/Li 2011.
830 LinkedIn is a business-related social network platform. URL: http://www.linkedin.com/.
831 Heuston 2011.
832 Thearling 2000.
833 Tan/Steinbach/Kumar 2006.
834 Madria/Bhowmick/Ng/Lim 1999.
835 Pamnani /Chawan 2010.
836 Schenker 2003.
837 Eirinaki/Vazirgiannis 2003.
838 Web content mining and web structure mining are applied on web documents such as web pages and therefore are less harmful from the privacy perspective.
839 Pamnani /Chawan 2010.

data that is collected implicitly, data mining also uses explicitly collected data, e.g. by registration forms in which the user enters his demographics or interests. Since web usage mining investigates the navigational behavior of an individual user, it can also be used for de-anonymization; that is discussed in the next section.

Generally, a data mining process includes data collection (data aggregation), pre-processing, pattern discovery, and evaluation.[840] Data collection has been discussed in the previous section. The pre-processing phase eliminates irrelevant data from the data set, for example by filtering irrelevant information. In the pattern discovery stage interesting navigation patterns of the corresponding user are discovered.[841] The pattern discovery phase includes classification, clustering, and prediction algorithms.[842] Finally in the evaluation phase, the predicted patterns are evaluated; for example, to evaluate future intent or action. An example of the purpose of applying data mining is when a company wants to find out, *why customers buy certain products*. In such a scenario, data mining may be applied on the purchase history and the data they have on the customers' interests and demographics.

De-anonymization and Re-identification

De-anonymization refers to linking/connecting of anonymized[843] data to an individual user, group[844] or to an identity. The basic method of database anonymization is to suppress, generalize, or replace the identifying attributes of a data record.[845] In Figure 2 the anonymization attempt by suppressing the attributes of the identities from the database is demonstrated. In this case, de-anonymization can be performed by combining the anonymized database with other databases. More advanced anonymization methods are group-based anonymization techniques, e.g. k-anonymity,[846] l-diversity, and t-closeness[847] which are discussed further in Section 4.4.1. However, even for such sophisticated anonymization methods, de-anonymization and privacy breaches have been discovered.[848,849,850] Generally, because only the directly identifiable attributes are removed from a database, the database cannot be considered to be anonymized; by re-identification the data can be still linked to a specific person.[851]

Figure 2: An example of a database and the attempts to anonymize it in order to provide privacy is demonstrated. (a) demonstrates the original database; the column marked in red contains the identity attribute (b) the identity attributes are suppressed from the database, however the other attributes can also link the diagnoses to the identities. The only way to provide privacy is to suppress every attribute except for the Zip code. However, in such a case the data loses its usefulness for research purposes.

(a)

NAME	NATIONALITY	BIRTHDAY	ZIP CODE	DIAGNOSE
Ben A.	USA	23/5/1980	455896	Flu
Sam S.	German	09/12/1972	623911	Heart Disease
Tom R.	UK	28/1/1976	455763	Diabetes
Kim I.	Japanese	17/3/1982	623911	Flu

840 Mobasher 2007.
841 Hu/Zong/Lee/Yeh 2003.
842 Chapple 2011.
843 "The term anonymous implies that the data cannot be manipulated or linked to identify an individual." Sweeney 1997.
844 Or outside information which is generally available to the public - collected on a daily or routine basis (such as voter registration information), and which includes identifying information [Epic on Re-identification]
845 Sweeney (1) 2002.
846 Sweeney (1) 2002, Sweeney (2) 2002.
847 Wong/Fu/Wang/Yu/Pei 2011.
848 Id.
849 Machanavajjhala /Gehrke /Kifer 2007.
850 Li/Li/Venkatasubramanian 2007.
851 Epic on Re-identification.

(b)

NATIONALITY	ZIP CODE	DIAGNOSE
USA	455896	Flu
German	455896	Heart Disease
UK	455896	Diabetes
Japanese	455896	Flu

4.3.3 LONG TERM STORAGE OF INFORMATION

Long term storage systems are systems in which data lifetimes exceed several decades. For example Electronic Health Records (EHR) might be stored in long term storage systems. The confidentiality risk for data that are stored on long term storage systems is unintentional disclosure, thus, threatening the self-determination right. Data confidentiality of a storage system is commonly guaranteed by encryption.

The security of current encryption methods, however, are not designed for long periods such as several decades. Thus, the confidentiality of long term storage systems cannot be guaranteed.[852,853] Concrete security of cryptosystems is based on the current infeasibility of a specific computational hardness of problems, and the hardness of such problems is often not proven. With advances in technology and cryptanalysis, solving such problems will be feasible in the long term, and hence most cryptosystems in use will become insecure. Additionally, since the data keeper or data controller will probably not be the same during the entire lifetime of the data, long term storage systems are also prone to inadvertent disclosure. In addition, organizational, political, and technological changes in the long term might lead to data leaks. The persistence of data on the web (i.e. data that was shared on OSNs) also might lead to long term storage. Moreover, long term storage systems may contain data on a person's past interests, state, and records, which might be no longer accurate. One may not want his future employer to have access to his past social network or newsgroup posts. Hence, long term storage of data affects the user's control over his data and leads to weakening the self-determination right.[854]

4.4 EXISTING TECHNICAL SOLUTIONS

To cope with the previously discussed privacy-threatening techniques on the internet and to tackle the problem of internet privacy, this section gives an overview of currently existing technical solutions for establishing a culture of privacy on the internet.

In order to structure the plethora of different approaches and technical solutions that enhance privacy on the internet, this section is organized in a way that was inspired by the layered structure of the ISO/OSI reference model.[855] We therefore start with a section on basic privacy enhancement principles that form a common theoretical background for the subsequently introduced techniques and solutions. These techniques are then presented in four sections: the Application Level, the Middleware and Network Level, the Infrastructure Level, and Combined and Integrated Solutions.

We deliberately make simplifications wherever suitable, discarding technical details, only mentioning the main and, in our opinion, most popular technological representatives as examples for underlying function principles.

4.4.1 THEORETICAL FOUNDATIONS AND CONCEPTS

This section introduces basic terms, concepts, and foundations that are common for many of the technical solutions presented in the subsequent sections.

852 Buchmann/ May/Vollmer 2006
853 Baker/Shah/Rosenthal/Roussopoulos/Maniatis/Giuli/Bungale 2006.
854 Head/Yuan 2001.
855 Zimmermann 1980.

Cryptography

Since many of the technical solutions presented in this work make use of cryptography, we introduce the most fundamental concepts in this area. Cryptography is defined as "the study of mathematical techniques related to aspects of information security such as confidentiality, data integrity, entity authentication, and data origin authentication".[856] It may therefore not only be used to prevent data disclosure, but also to detect cheating and other malicious activities. In the following, we discuss the two main principles of cryptography: symmetric and asymmetric encryption.

In a symmetric-key encryption system (e.g. AES (Rijndael)[857], Blowfish[858]), two or more participants agree on one shared secret key that is used to both encrypt and decrypt confidential messages. A major issue of symmetric-key cryptosystems is the key distribution problem, since the shared symmetric key must be agreed upon and exchanged in a secure way before it can be used. Wi-Fi home networks are a practical example for symmetric cryptosystems: the owner of the network fixes a pre-shared secret key that must made known to each computer in order to be able to connect to the network.

In a public-key cryptosystem (e.g. RSA[859], ElGamal[860]), each user generates a computationally dependent keypair consisting of a public key and a private key. While the public key of each participant is publicly available, the corresponding private key must be kept secret. A message can then be sent confidentially by encrypting it using the public key of the recipient of the message. The message can then only be decrypted using the corresponding private key of the recipient. Additionally, public-key cryptosystems provide the possibility to sign messages and can therefore be used for sender authentication and non-repudiation. Although the two latter mechanisms seem to be conflicting with privacy, they are essential from a trust perspective. However, public-key cryptography comes with the problem of potential impersonation by adversaries. Therefore it is crucial to authenticate public keys in order to achieve data origin authentication of the public keys themselves;[861] the section on certification will address this problem.

Symmetric and asymmetric cryptosystems have a number of complementary advantages. Modern cryptographic systems exploit the strengths of each.[862]

Trust

Trust is a complex and ambiguously defined property. It is often referred to as the "belief in the honesty, truthfulness, competence, and reliability" of an entity (human individual, organization, technical device, etc.).[863] As consequence an entity can be considered trustworthy, "if it always behaves in the expected manner for the intended purpose".[864]

Despite the various definitions and aspects of the term trust, in this section we only investigate the role of trust and trust relationships with respect to privacy, as trust in many cases is a necessary property for ensuring privacy. Privacy can, for example, be seen under the precondition to trust the recipient of private data to not use or redistribute this data in a way that conflicts with the owner's intentions.

856 Menezes/Oorschot/Vanstone 1996.
857 Daemen/Rijmen 2002.
858 Schneier 1993.
859 Rivest/Shamir/Adleman 1978.
860 ElGamal 1985.
861 Menezes/Oorschot/Vanstone 1996.
862 Menezes/Oorschot/Vanstone 1996.
863 Grandison/Sloman 2000.
864 Rosteck 2008.

There exist a couple of different approaches and techniques to establish trust in the context of internet services. The following sections thus give an overview of the most important and established ones, presenting only a sampling of what is possible.

> Certification

One of the most popular approaches to establish trust relationships on the internet is the concept of (digital) certificates. These certificates are usually based on public key cryptography and their purpose is to ensure the binding between documents and "physical entities" such as human individuals or organizations".[865] Normally, certificates, e.g. X.509 certificates,[866] contain properties that identify the to-be certified entity, such as the name or an email address, and the public key of this entity. In addition to that, a certificate usually includes information about the issuing external authority and the validity of the certificate. By signing this information with its private key, the issuing authority generates a digital signature, which expresses that the authority verified the binding between the entity's identifying properties and its public key.

In case a third party wants to check the validity of the certificate, it needs to verify the digital signature within the certificate by using the public key of the issuing authority. If the third party trusts the issuing authority, it can find out whether a message signed with the private key of the entity to whom the certificate belongs is authentic or not, as the signature guarantees non-repudiation and integrity of the certificate.

To establish this chain of trust, this model of hierarchical certifications requires an established Public Key Infrastructure (PKI), with trusted third parties (called Certification Authorities (CA)) such as governmental organizations (e.g. Bundesnetzagentur as German root CA)[867] or private institutions (e.g. VersiSign). Although the common understanding of trust is usually not considered transitive,[868] this kind of certification is to some extent based on a transitive trust model.

Certificates are only useful in that they can for example be used to establish a trust relationship between the recipient and the sender of a signed message, if the recipient trusts the issuer of the sender's certificate. The usage of hierarchical certifications seems to conflict with the concept of privacy, as the main purpose of a certificate is the verified binding of an entity to its certificate by an external authority, which as a consequence always knows all these bonds.

An alternative to the model of hierarchical certification and trust relationships is the idea of a web of trust,[869] for example used by Pretty Good Privacy (PGP),[870] where no central certification authorities and thus no PKIs are needed, but the authenticity of the bond between public key and entity is established by cross certifications. Cross certification hence refers to a pair-wise verification procedure instead of a centralized one.

> Reputation and Reputation Systems

The concept of reputation is highly connected with trust and trustworthiness. Reputation is a "fundamental concept in many situations that involves interaction between mutually distrusting parties"[871] and can be seen as a "trust-enforcing, deterrent, and incentive mechanism to avoid cheaters and frauds".[872] Communication and interaction on the Internet, especially the use of web services such as e-commerce or auction systems, often lacks the applicability of traditional

865 Canetti 2004.
866 http://tools.ietf.org/html/rfc2510.
867 http://www.gesetze-im-internet.de/bundesrecht/sigg_2001/gesamt.pdf.
868 Gerck 2002.
869 Abdul-Rahman 1997.
870 Zimmerman 1995.
871 Shmatikov/Talcott 2005.
872 Sabater/Sierra 2005.

trust models.[873] Thus sometimes artificially-generated trust relationships are necessary to substitute the lack of trust cues, due to the lack of face-to-face contact. Online reputation systems, such as eBay's user rating system,[874] TrustRank,[875] or Google's PageRank system,[876] try to close this gap by acting as "adequate online substitutes for the traditional cues for trust and reputation".[877]

The main functional principle of such reputation systems is to infer reputation, and thus indirectly trust, based on metrics such as links to a particular web site, or subjective evaluations of a particular product.

While these reputation systems in most cases serve their purpose to establish a subjective level of trust, it is questionable whether the generated trust relations really correlate to real-world trust models. Additionally, online reputation systems are known to be prone to attacks on their integrity and to fraud in general.[878]

> Privacy Seals

In contrast to digital certificates that guarantee the authenticity of an entity, in particular that of a specific web site or service, Privacy Seals are meant to demonstrate trustworthiness with respect to given privacy statements and promises. This means that the issuers of Privacy Seals such as TRUSTe[879] or EuroPriSe[880] certify that specific websites' or web services' business processes correspond to their stated privacy policies, and that the collection and processing of private data does not violate these policies. This certification is usually based on audits of the corresponding business processes. This procedure is also a point of criticism, as it is often entirely based on audits which took place before the Privacy Seal was issued and then are renewed in periodic intervals. Active and automated detections of policy violations and thus violations of the Privacy Seal contract are seldom applied. Therefore, the Privacy Seal only reflects the privacy situation at the moment in time when the audit took place. As the corresponding business processes may change after the audit, a Privacy Seal may falsely indicate a trustworthiness and compliance with given privacy statements.[881]

Anonymity, Unlinkability, and Pseudonymity

The concepts of anonymity, unlinkability, and pseudonymity are closely connected to recent discussions about internet privacy, as most considerations about privacy demand a minimum level of anonymity or pseudonymity.[882] The remainder of this section gives an overview and presents suitable definitions of the corresponding terms.

> Anonymity

According to the Common Criteria, as stated within the ISO/IEC 15408 standard, anonymity "ensures that a user may use a resource or service without disclosing the user's identity"[883,884]. More precisely, anonymity can be considered as "the state of being not identifiable within a set of subjects, the anonymity set"[885]. This means that anonymity refers to an entity, as member of a set of entities, who cannot easily be identified and uniquely distinguished from the other members of that set. These somewhat blurry

873 Mui/Mohtashemi/Halberstadt 2002.
874 Resnick/Kuwabara/Zeckhauser/Friedman 2000.
875 http://www.trustrank.org/.
876 Page/Brin/Motwani/Winograd 1998.
877 Josang/Ismail/Boyd 2007.
878 Douceur 2002.
879 http://www.truste.com/consumer-privacy/.
880 https://www.european-privacy-seal.eu/.
881 Edelman 2009.
882 Pfitzmann/Hansen 2010.
883 http://www.commoncriteriaportal.org/files/ccfiles/CCPART2V3.1R2.pdf.
884 http://webstore.iec.ch/preview/info_isoiec15408-2%7Bed3.0%7Den.pdf.
885 Pfitzmann/Hansen 2010.

definitions of anonymity lead to the conclusion, that anonymity properties are very context-dependent and, in most cases, cannot be precisely quantified.[886,887] To tackle the problem of quantification of anonymity and to come up with a more precise notion, there exist several more formal approaches of describing anonymity. As the naive idea of an anonymized data set (a data set lacking directly identifying attributes) does not provide a sufficient level anonymity in practice (cf. 4.3.2.2), more sophisticated anonymity models are necessary.

Based on the conclusion that the sole removal of uniquely identifying attributes within a data set does not provide a sufficient level of anonymity, Sweeney states that a data set is considered to provide anonymity, if it fulfils the k-anonymity property.[888] A data set, containing information about k entities, fulfils the k-anonymity property, if and only if the information of each entity within the set cannot be distinguished from the information of at least k-1 entities within this set. This in less formal words means, that a data base is k-anonymous, if each entry is identical with at least k-1 other entries. Identical in this terms means, that all attributes of the entries are generalized until the entry does not differ anymore from the other k-1 entries.

Although the k-anonymity approach offers a formalized way to provide some anonymization guarantees, it is prone to several attacks that in some cases are capable of destroying anonymity even if a data set fulfils the k-anonymity property; for example if the attributes within the data set have little diversity.[889,890,891,892]

To cope with these limitations of the k-anonymity approach, Machanavajjhala et al. proposed the l-diversity criterion.[893] The concept of l-diversity is based on the observation, that the distribution and diversity of attributes within a data set significantly influences the possibility for successful attribute disclosure attacks. The l-diversity principle thus demands a high diversity of sensitive attributes to reduce the possibilities for an attacker to infer sensitive information due to additional knowledge from external sources. Furthermore, each set of sensitive attributes (e.g. all real names, phone numbers, etc.) must have at least l well-represented value for all possible sensitive attributes. The term "well-represented" in this definition is not explicitly defined, therefore the authors propose a couple of different means to establish this "well-representedness" by defining constraints on the distribution of the sensitive attributes.[894]

Recent studies show, that the l-diversity approach still has limitations due to necessary assumptions about attacker knowledge and in that it suffers from several weaknesses that can be exploited to launch attribute disclosure attacks. Li et al. therefore introduced the anonymity concept of t-closeness. Similar to l-diversity, t-closeness addresses the problem of diversity of sensitive attributes, but instead of analysing the distribution independently for each equivalence class, t-closeness "requires that the distribution of a sensitive attribute in any equivalence class is close to the distribution of the attribute in the overall table". The authors claim, that t-closeness outplays l-diversity in terms of attribute disclosure.[895]

886 Pfitzmann/Hansen 2010.
887 Zarsky 2004.
888 Sweeney 2002.
889 Diversity here refers to the number of different attribute values.
890 Sweeney 2002.
891 Machanavajjhala/Kifer/Gehrke/Venkitasubramaniam 2007.
892 Li/Li/Venkatasubramanian 2007.
893 Machanavajjhala/Kifer/Gehrke/Venkitasubramaniam 2007.
894 Li/Li/Venkatasubramanian 2007.
895 Li/Li/Venkatasubramanian 2007.

In summary, the above-mentioned approaches of establishing and ensuring anonymity for data sets strengthens the possibility of successful de-anonymization of (statistical) data bases and thus to re-identify particular identities (cf. 4.3.2.2).

> Unlinkability

The property of unlinkability is closely connected to anonymity, as unlinkability is a sufficient condition for realizing anonymity.[896] The ISO/IEC 15408 standard defines unlinkability as a property that "requires that users and/or subjects are unable to determine whether the same user caused certain specific operations".[897,898] Pfitzmann et al. argue that unlinkability only has a meaning, if the system for which anonymity or unlinkability should be defined, has been sufficiently described. This means that all entities that are potentially interested in linking different items of interest have to be described.[899] Therefore "unlinkability of two or more items of interest means that within the system, from the attacker's perspective, these items of interest are no more and no less related after his observation than they are related concerning his a-priori knowledge".[900]

This more attacker-centred definition allows anonymity to be described as the unlinkability of an item of interest and any subject in the context of the system under observation. Therefore, in the context of internet privacy, we can say that a high level of unlinkability leads to a high degree of anonymity, and thus, as stated above, usually correlates with a high level of privacy.[901,902]

> Pseudonymity

Pseudonymity and anonymity are similar concepts in that both aim at protecting an entity from having its identity revealed. But while true anonymity necessarily requires unlinkability between an entity and the corresponding items of interest, the concept of pseudonymity explicitly requires a linkage between a pseudonym and the respective items of interest. The ISO/IEC 15408 standard states, that pseudonymity "requires that a set of users and/or subjects are unable to determine the identity of a user bound to a subject or operation, but that this user is still accountable for its actions".[903,904]

This means, that a pseudonym is bound to an entity and all items of interest subsequently linked to this pseudonym. The knowledge of the connection between the pseudonym and the corresponding entity would thus allow full linkage of all items of interest to this particular entity. The benefit of this concept, compared with true anonymity, is that it provides means to allow accountability, which is not possible within the concept of anonymity.[905,906] The selection of appropriate pseudonyms is crucial for real pseudonymity, as pseudonyms that allow inferences on the entity's identity may lead to a linking of the respective items of interest. Whether pseudonymization and anonymization really guarantee privacy is subject to controversial discussions and, at least for currently available implementations, proven to be insufficient.[907,908]

896 Pfitzmann/Hansen 2010.
897 http://www.commoncriteriaportal.org/files/ccfiles/CCPART2V3.1R2.pdf.
898 http://webstore.iec.ch/preview/info_isoiec15408-2%7Bed3.0%7Den.pdf.
899 Pfitzmann/Hansen 2010.
900 Pfitzmann/Hansen 2010.
901 Pfitzmann/Hansen 2010.
902 Steinbrecher/Koepsell 2003.
903 http://www.commoncriteriaportal.org/files/ccfiles/CCPART2V3.1R2.pdf.
904 http://webstore.iec.ch/preview/info_isoiec15408-2%7Bed3.0%7Den.pdf.
905 http://webstore.iec.ch/preview/info_isoiec15408-2%7Bed3.0%7Den.pdf.
906 Pfitzmann/Hansen 2010.
907 Rao/Rohatgi 2000.
908 Steinbrecher/Koepsell 2003.

Differential Privacy

The original incentive for coming up with the concept of differential privacy came from the context of preserving privacy within statistical databases.[909] To generate a statistical database out of a database that contains potentially sensitive entries which should not be made public, the data provider has to somehow sanitize the data records itself in a way that no confidential data is included afterwards. The previously introduced anonymity concepts: k-anonymity, l-diversity, and t-closeness, all define properties on the distribution of entries and structure of a database itself. In contrast to them, the concept of differential privacy specifies a property on the release function[910] of a database. The necessity of said property was the consequence of a proof, that any statistical database with a non-trivial utility necessarily compromises privacy.[911]

A random release function satisfies ε -differential privacy, if the presence of one more entry in the input data set does not significantly influence the likelihood of the function's output. As consequence, the joining or leaving of an entity to a statistical database should not add (significant) additional risk to the entity's privacy.

In a nutshell, one of the main ideas of the concept of differential privacy is to shift the focus of the discussion about preserving privacy from reasoning about the additional knowledge an adversary gets from data records to whether or not the pure presence of an individual in a database increases its privacy risk.[912]

Identity Management

A person's identity is a complex and hard to define entity. Name and home address, social security number, or passport ID are typical and well-known parts of an identity that can be used to precisely identify a particular person. But an identity consists of more than just such hard facts and numbers. Personal preferences such as hobbies, nicknames, and music interests are less concrete and thus harder to be measured and stated precisely. Nevertheless such attributes are also parts of our identity and describe us in some cases even better than hard facts such as our social security number. In all cases where persons reveal personal information, this information is not complete and does not cover the complete identity. Thus we speak of partial identities as subsets of a person's complete identity.[913]

For reasons of identification and authentication, information systems depend on the elicitation, storage and processing of such partial identities. This often creates a conflict, as many information systems, such as web services, need to know such information, while users may for reasons of privacy want to avoid this revealing of their identity, or at least restricting the disclosure to the bare minimum.[914]

Identity management systems try to tackle this problem by providing means to manage multiple partial identities in order to always only reveal as much information about a person's identity as absolutely necessary to perform a particular task. Identity management systems thus aim at minimizing the amount of personal data that is revealed to third parties. A social networking service for example is highly interested in eliciting and inferring as many parts of a user's identity as possible, as its business model highly depends on the amount of collected data. But in order to be utilized by a particular user, only a very limited subset of this person's identity is actually required.

---

909 A statistical database consists of sensitive information from a large number of respondents (e.g. all tax payers), with the goal of learning and releasing to the public corresponding statistical facts.

910 The release function is the mechanism that anonymizes the entries within a normal database to generate an anonymized statistical database.

911 Dwork 2008.

912 Dwork/Smith 2009.

913 Clauss/Koehntopp 2001.

914 Hansen/Schwartz/Cooper 2008.

The social networking service Facebook, for example, only requires a user to provide her name, surname, email address, and a password, to allow the usage of its services. These data, from the technical point of view, do not necessarily have to be correct in a way so that it corresponds to the real identity of the user. Therefore users, in order to preserve their privacy, may provide only partial, maybe even incorrect parts of their identity to the service.

Identity management systems such as iJournal,[915] the identity management part of the MozPETs framework, or iManager[916] try to enhance privacy by minimizing the disclosure of private data and therefore reducing linkability. In the particular case of reducing the amount of personal data that is disclosed when creating an account for an online social network, identity management systems can assist the user. This can for example be done by only providing as little of his real identity as absolutely necessary to use the service, generating an adequate pseudonym that does not directly reveal any personal information, and filling the rest of the application form with fake information.

To maintain the mapping of the user's real identity and the fake information for that particular service, the identity management system then stores this information and offers the user a possibility to reuse it, whenever the service is used again.

Access Control and Usage Control

The goal of access control is to constrain what users and programs executing on their behalf are allowed to do; it therefore seeks to prevent activities that could lead to security breaches.[917] For this reason users are assigned permissions on specific objects. A so-called reference monitor mediates any attempted access on objects and determines, based on the assigned rights, whether the access is to be allowed or blocked. A prerequisite for access control is that users have successfully been authenticated prior to access control enforcement.[918]

In role-based access control (RBAC),[919] administrators create roles according to job functions performed in an organization and assign permissions to these roles rather than users. Users are then assigned to roles on the basis of their competences and responsibilities and "inherit" the permissions of the corresponding roles. Yet, "conventional access models [. . .] don't enforce privacy policies and barely meet privacy protection requirements",[920] the reason being that standard access control systems do not provide the property of purpose-binding which is often necessary in a privacy context.[921] Privacy-aware role-based access control (P-RBAC)[922] therefore attempts to support privacy policies by extending RBAC to include the intended purpose, conditions, and obligations under which an attempt at access is granted.

Usage control goes beyond traditional access control[923] by "controlling not only who may access which data, but also how the data may be used or distributed afterwards".[924] Usage control introduces, among others, the concept of obligations that restrict the future usage of data. By defining usage control policies, data providers can control how and under which circumstances their data may or may not be used by potential data consumers. Yet, ensuring the

915 http://mozpets.sourceforge.net/.
916 Jendricke/Markotten 2000.
917 Sandhu/Samarati 1994.
918 Sandhu/Samarati 1994.
919 Sandhu/Coyne/Feinstein/Youman 1996.
920 Ni/Bertino/Lobo/Calo 2009.
921 Powers/Ashley/Schunter 2002.
922 Ni/Bertino/Lobo/Calo 2009.
923 Park/Sandhu 2002.
924 Hilty/Pretschner/Basin/Schaefer/Walter 2007.

compliance of a data consumer with usage control policies is only possible if the data consumer's system is trusted. An exemplary application of usage control mechanisms for purposes of increasing privacy in the internet is the problem of long term storage of data (see Section 4.3.3). By defining usage control obligations like "data must be deleted within 30 days" it is possible to define artificial expiration dates on data to for example prevent personal data to be stored arbitrarily long in a way that was not intended by the owner. However, defining and enforcing such obligations is still a challenging, and partially not yet solved, task.

While traditional access control is implemented in nearly any domain, privacy-preserving mechanisms like P-RBAC are rarely deployed. Yet, any access control mechanism fails to protect data once access has been granted. The comparatively young research field of usage control tries to close this gap; however, the concept is not yet ready to be deployed.

4.4.2 APPLICATION LEVEL

Privacy Policy Languages

In today's internet environment, privacy policies that inform the user about data collection and usage within the context of a web site or service are often only presented in the form of legal documents. These documents are usually written in a way that is hardly understandable for the average user and also not machine-readable and thus not automatically processable. As a consequence, privacy policy statements are often either misunderstood by users or even not read at all.[925] To cope with this problem and to support the user by means of automated policy evaluation, a couple of machine-readable privacy policy standards were introduced.

The Platform for Privacy Preferences (P3P) is a web protocol that was designed "to inform Web users about the data-collection practices of Web sites".[926] Primarily, P3P was developed to improve the trust relationship between web site and user by informing the user about to-be collected data and thus enabling a more precise control regarding the disclosure of private data. To that end, P3P offers the possibility to encode privacy policies in a machine-readable manner that can automatically be processed by P3P compatible software. Privacy policies in this context refer to statements about a website's data management and privacy practices. This includes, among others, the data that is collected, its type, the purpose and intended usage of the collection, and the permanence and visibility of the to-be collected data. Based on these privacy policies the user can then decide upon visiting the web site, whether to pass this data to the web server, to only partially allow the transfer, or to completely deny the collection of private data. This is done by comparing the privacy preferences of the user and the privacy policies of the web site. For exchanging privacy preferences between user agent and web site, W3C proposed the APPEL language,[927] which allows the user to specify a set of user privacy preferences, the so-called rule-sets, in a structured way. These rule-sets can then be used by web browsers and matched against server privacy policies. There exist a couple of reference implementations of the P3P protocol, including P3P compatible web browsers and P3P browser extensions. As the P3P protocol does not explicitly state how to enforce these policies and how to proceed in case of a policy violation, these implementations differ in terms of possibilities for user interaction and the degree and nature of the used enforcement mechanisms. Since version 6.0 Microsoft Internet Explorer partially supports P3P, in that it allows the display of the P3P policies of a website and matches these policies against the configured user privacy settings. Currently the only possibility to react on mismatching policies is to deny the transfer of cookies. Mozilla Firefox also supports cookie handling based on P3P policies since version 1.5.

925 Cranor/McDonald/Egelman/Sheng 2007.
926 http://www.w3.org/TR/P3P11/.
927 http://www.w3.org/TR/P3P-preferences/.

In addition to this limited built-in P3P browser support, browser plug-ins like Privacy Fox for Mozilla Firefox,[928] or Privacy Bird for Microsoft Internet Explorer,[929] offer a more comprehensive P3P support. This for example refers to automated translation support between P3P policies and a user-understandable natural language format and a wider range of enforcement and interaction possibilities.

Although there currently exist a wide range of technical solutions for implementing P3P, it never reached a wide acceptance, either at the data provider side (web sites) or at the data consumer side (web users).[930]

The eXtensible Access Control Markup Language (XACML) was not primarily designed as privacy policy language, but as means to express access control restrictions at the level of individual attributes, such as for example patient records in a hospital database context. As the concept of denying or allowing access to particular data items by defined subjects, based on a pre-defined rule set, closely relates to the intention of Privacy Policies, XACML can also be used to express privacy policy statements.[931] One of the benefits of using XACML as privacy policy language is that there already exist implementations and solutions to evaluate and enforce such policies within an information system. In addition to that, XACML also offers some more advanced policy features, such as the specification of obligations or the delegation of rights. XACML nevertheless exhibits some limitations, as there for example still exist issues in automatically analysing complex policies with respect to consistency, correctness, or introduced conflicts, due to the comparably rich expressiveness of the language.[932]

Privacy Icons

The purpose of Privacy Icons is to provide a user-friendly and user-understandable way of providing information about the usage of private data within a web site or web service. This is, for example, achieved by representing usually complex and hard to understand privacy policies in the form of self-explanatory pictures. The main reason is that privacy and data usage policies are quite often either written in legalese, incomprehensible to an average user, or in the more rare cases, only available in a machine-readable and thus not easily human-understandable format. Approaches like the Mozilla Privacy Icons project thus have the intentions of "creating a simple standard to explain privacy policies" and "to enable web users to make better choices when picking and using web services".[933] While Privacy Icons may have great potential to make privacy policies more accessible and thus users more aware of potentially unwanted data collection and processing, there are a couple of arguments against their usefulness. Hansen[934] for example claims, that companies that are intending to use collected data for commercial purposes, e.g. by selling data records to email advertisement services, will most likely either not put the negative "Your data may be sold" pictogram on their webpages, or even intentionally use the wrong signs. Due to the fact that the usage of Privacy Icons is currently not legally binding, there is basically no way to enforce their correct usage. Therefore the trustworthiness of Privacy Icons is at this time not at all guaranteed and their usefulness in terms of increasing privacy at least arguable.

Clear, transparent, reversible Procedures

Addressing the issues concerning transparency, accountability, and reversibility of the usage of private data on the internet, privacy-centric data usage procedures have

928 Arshad 2004.
929 Cranor/Arjula/Guduru 2002.
930 Cranor/McDonald/Egelman/Sheng 2007.
931 http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=xacml.
932 Kolovski/Hendler 2007.
933 https://wiki.mozilla.org/Drumbeat/Challenges/Privacy_Icons.
934 Hansen 2009.

become means to support the attempts to increase privacy and thus user trust in internet services.

One popular approach to increasing transparency regarding the usage of private data by web sites and internet services is the concept of Privacy Dashboards. Privacy Dashboards like the Google Dashboard[935] or the W3C Dashboard proposal[936] strive to let users know about the amount, type, and optionally the intended usage of the private data. Google Dashboard informs the users about the data Google has collected about them. Yet, the presented data sets are incomplete, as they e.g. do not contain any information about user tracking activities. Hence, Privacy Dashboards often raise criticism concerning the completeness, correctness, and consistency of the presented data. This leads to the conclusion that Privacy Dashboards may increase the perceived privacy, but whether they really increase transparency is questionable. Techniques like Privacy Evidence extend the idea of increasing transparency by informing users about stored and processed data by introducing additional auditing and policy compliance mechanisms.[937] By this means, users can not only see which data is maintained and processed by a web site or service, but also to what extent the collection and usage is done with respect to user- or service-defined policies and regulations. To do so, these techniques often make use of secure logging and automated audits of the correctness of these logs, which to some extent assure the integrity and credibility of the performed compliance checks.

The Transparent Accountable Datamining Initiative (TAMI) approach[938] has a slightly different scope. Due to the observation that simply controlling access to data is no longer adequate in terms of protecting user privacy, the authors propose to focus on the usage aspects of data rather than on pure data access restrictions. This should primarily be achieved by making the web in some sense policy-aware, in a way that allows for an accountable and transparent usage of data. Weitzner et al.[939] thus propose the Policy Aware Web infrastructure, a solution which combines the usage of data with usage constraints and a means to audit and ensure the proper adherence to these constraints. Although the TAMI approach is highly tailored to fit a scenario where law enforcement agencies desire to use data mining techniques for criminal investigation purposes, the insights and mechanisms of this approach can be transferred to any other situation that requires for provable accountability and transparency properties on large data sets. The TAMI approach aims at regulating the usage of data in a way that prohibits "actions premised on factual incorrect antecedents", "impermissible sharing of data beyond the collecting organization", and "actions premised on interference from data that [...] is used for an impermissible purpose".[940] In summary, TAMI is about the idea of introducing restrictions on data mining techniques, in order to control what is allowed to be gathered, processed, and used for inference purposes (see Section 4.3.2.2).

Private Credentials

Private Credentials, or Minimum Disclosure Tokens, are credentials that "let individuals prove their authorization without revealing information that might identify them".[941] Thus the concept of Private Credentials relates to the security property of unlinkability, which requires that the information contained in the credentials themselves does not allow the deduction of any additional information about the identity of the corresponding user.[942] Private Credentials

935 https://www.google.com/dashboard/.
936 http://code.w3.org/privacy-dashboard/.
937 Sackmann/Strücker/Accorsi 2006.
938 Weitzner/Abelson/Berners-Lee/Hanson/Hendler/Kagal/McGuiness/Sussman/Waterman 2006.
939 Weitzner/Abelson/Berners-Lee/Hanson/Hendler/Kagal/McGuiness/Sussman/Waterman 2006.
940 Hedbom 2009.
941 Hansen/Schwartz/Cooper 2008.
942 Steinbrecher/Koepsell 2003.

can therefore be seen as the digital equivalent to real-world authorization stamps or non-personalized tickets, which authorize persons without revealing their identity. There have been some attempts to deploy the concept of Private Credentials in a real-world context, such as the PrivateCredentialPermission class within the JavaSE framework, or the open-source digital payment project OpenCoin.[943]

Privacy enhanced Browsing

As already described before, there exist some approaches to address privacy concerns at the level of web browsers. The P3P plug-ins PrivacyBird or PrivacyFox enhance the browser functionality with means to control the granularity and amount of private data that is leaked upon visiting a web site or using a web service. Apart from these P3P implementations there exist approaches to directly integrate privacy-enhancing mechanisms into web browsers by design. The main design goal of the Mozilla Privacy Enhancement Technologies (MozPETs) project is to include "as many privacy enhancement technologies (PETs) as possible".[944,945] This includes, among others, the integration of TOR and JAP support, the introduction of special Privacy Icons, or mechanisms to block potentially privacy-threatening techniques such as web bugs (cf. Section 4.3.1). Microsoft Research's RePriv browser project is a "browser-based technology that allows for Web personalization, while controlling the release of private information within the browser".[946] The main intention behind this project is to cater to the impression that users want both a highly personalized web experience and a high level of privacy. Therefore, RePriv collects data about user preferences and main interests by observing the user behaviour, and offers the user the possibility to individually decide, whether this data is allowed to be propagated to a web site or service. Due to that, the authors of RePriv state that combined local data mining and selective data disclosure allow RePriv to offer a reasonable trade-off between privacy and usability.[947]

In addition to these privacy-centred browsers and plug-ins, there exist a couple of plug-ins and browser extensions that were not primarily designed as privacy-enhancing techniques, but nevertheless are capable of increasing user privacy to some extent. Popular examples of this category are NoScript,[948] a browser extension that allows selective blocking of client-side content such as JavaScript, Java, and Flash; Bugnosis,[949] a tool to identify web bugs within a website and thus raise privacy awareness; or the Target Advertising Cookie Opt-Out (TACO) extension[950] to opt-out of tracking networks by blocking specific cookies (this relates to the threat of tracking user behaviour by the use of cookies – see Section 4.3.1). The Privacy Mode offered by most modern browsers cannot directly be considered privacy-enhancing, as it mainly focuses on local mechanisms such as disabling the browsing history, and reducing local traces of the web surfing behaviour of a user. While these methods may increase the local privacy of a user, they are not capable of preventing the unintended leakage of private data to web sites or services. Nevertheless, the often included cookie blocking may act as a means to support privacy enhancing attempts.

4.4.3 MIDDLEWARE AND NETWORK LEVEL

Proxy servers

A proxy server is a server in the form of a hardware system or an application that acts as an intermediate when

943 http://opencoin.org/.
944 Brueckner/Voss 2005.
945 http://research.microsoft.com/en-us/projects/repriv/.
946 http://research.microsoft.com/en-us/projects/repriv/.
947 http://noscript.net/.
948 Alsaid/Martin 2002.
949 http://www.abine.com/preview/taco.php.
950 http://www.pps.jussieu.fr/~jch/software/polipo/.

resources like a web page are requested and/or returned. There exist different proxy servers for different kinds of communication protocols (e.g. HTTP) that can be used, among other things, for access control, content filtering, and logging. When set up accordingly, proxy servers can increase the privacy of internet users and allow for anonymous access to web resources. There exist numerous HTTP proxies, both application-based and web-based.

Application-based proxy servers (e.g. Polipo[951], Privoxy[952]) are usually installed on the user's machine and act as an intermediate for applications like the web browser. After the application has been configured to use the proxy, all internet traffic of this application will be mediated through the proxy and handled according to the proxy configuration. This includes the possibility to strip personally identifying protocol headers (e.g. Referrer, User-Agent), to read and/or set cookies, and to block potentially dangerous content like JavaScript code or Flash snippets.

Web-based proxy servers (e.g. Anonymouse[953], ProxFree[954]) provide the user with an easy-to-use web interface; they relay the messages of the user and are mainly used to browse anonymously. Depending on the proxy, they may, either through user configuration or by a default rule set, strip HTTP headers (e.g. information that could be used to generate fingerprints and thus may be used to identify a particular user – see Section 4.3.1) and/or potentially dangerous content like JavaScript. Proxy.org[955] maintains a comprehensive list of web-based proxy servers.

Application-based proxies are usually hard to configure properly, especially for average internet users, since an overly lax configuration results in revealing too much personal information, while overly restrictive settings render web applications useless. Furthermore, these kinds of proxies cannot provide anonymity at the layer of IP addresses (cf. Section 4.3.1). Yet, in contrast to web-based proxies, the use of application-based proxies does not result in communication overhead and no proxy provider needs to be trusted, since the proxy is run by the user herself. Web-based proxies need not be configured by the user and are rather self-explanatory and user-friendly. They can provide anonymous web access for the user at the cost of communication overhead and the need to trust the proxy.

Network Layer Traffic Protection

Network communication is organized in several layers that build upon on one another.[956] Network traffic can therefore be protected at several layers, e.g. on the presentation layer (TLS), the transport layer (Tcpcrypt), or the network layer (IPsec). Design goals of these protocols include confidentiality and integrity of data, therefore providing "improved privacy, reduced risk of sensitive information leakage, and greatly reduced ability [...] to monitor all traffic without being detected".[957]

The Transport Layer Security (TLS) Protocol[958] builds upon the transport layer and is therefore transparent for application-specific protocols (like HTTP for web browsing). TLS allows for the authentication of the communication partners by means of asymmetric cryptography. After establishing a symmetric key in an initialization phase, TLS provides confidentiality and integrity. Well-known applications than can be used via TLS include web browsing[959]

951 http://www.privoxy.org/.
952 http://www.anonymouse.org/.
953 http://www.anonymouse.org/.
954 https://www.proxfree.com/.
955 http://www.proxy.org/.
956 Zimmermann 1980.
957 Bittau/Hamburg/Handley/Mazieres/Boneh 2010.
958 Dierks/Rescorla 2008.
959 Rescorla 2000.

and email.[960,961] Although TLS is application-protocol independent, applications (e.g. web server, internet browser, email server, or email client) must be designed to support TLS. There exist several frameworks to allow application programmers to easily integrate TLS support into their application (e.g. OpenSSL[962], GnuTLS[963]).

IPSec[964] addresses security at the network/IP layer, and offers among other benefits, integrity, data origin authentication, access control, and confidentiality. Since IPsec operates at the IP layer, these security services are provided "in a standard fashion for all protocols that may be carried over IP".

Tcpcrypt[965] is a standard draft providing an extension for TCP and therefore tackling traffic protection at the transport layer. The authors' goal is to make end-to-end encryption on the internet the default by also supporting legacy applications not originally designed for encryption and integrity checking.

Network layer traffic protection is a well-understood field and provides solid means to protect users' privacy on the internet. The unnoticed analysis of the communication between users and web services, which highly affects user privacy, is significantly strengthened (see Section 4.3.2.1), although, due to the computational expense of traffic protection, especially on the server's side, these mechanisms are rarely used in scenarios other than online banking or e-commerce.

Mix cascades and mix networks

Chaum[966] lays the foundations for techniques that allow for anonymous and confidential communication on the internet using public key cryptography. The approach makes use of so-called mixes - computers that relay messages, hiding the correlation of the messages in its input and those in its output by means of cryptography (basically a decryption) and reordering the messages. In order to send an anonymous and confidential message, the sender first encrypts the message with the public key of the receiver and then with the public key of the relaying mix. If the relaying mix operates correctly, a network observer cannot relate the messages sent to and the messages sent from the mix, therefore hiding any user of the mix within all other users using this mix in a certain time interval. In order to prevent attacks that are based on sending the same message more than once (replay attacks), a mix must ensure that no message is relayed twice. Furthermore, users must send dummy traffic when not communicating, in order to defend against attackers that are able to observe the network globally. These methods increase the steps an attacker has to take in order to link activities to one particular identity (i.e. identifying the IP address of an end-user – see Section 4.3.1).

Since the usage of one single mix allows for linking the two communication partners by the mix itself, Chaum proposes a cascade of mixes. "Any single constituent mix is [then] able to provide the secrecy of the correspondence of the entire cascade".[967] The sender then needs to encrypt the message successively for the receiver and each mix in the cascade. Communication using Chaum mixes is by default unidirectional. In order to allow for a response without revealing her identity, the sender has to ship an encrypted return address along with the message. Using the concept of a set of mixes, there is no need for a universally trusted party, since any single constituent mix is sufficient to provide anonymity. When using mix cascades, the series of mixes to

960 Hoffman 2002.
961 Newman 1999.
962 http://www.openssl.org/.
963 http://www.gnu.org/software/gnutls/.
964 Kent/Seo 2005.
965 Bittau/Hamburg/Handley/Mazieres/Boneh 2010.
966 Chaum 1981.
967 Chaum 1981.

use is fixed in advance and Chaum's concept assumes that any mix can communicate with any other mix. In contrast, mix networks do not fix the mixes in advance but each user chooses a set of mixes individually. Therefore it is the user's responsibility to choose at least one constituent mix that provides the anonymity for the communication.

Onion routing[968,969] is a general-purpose infrastructure for anonymous and confidential communication over a public network, e.g. the Internet. It makes use of numerous distributed Chaum mixes under the control of different administrative domains. These mixes are connected by permanent connections and the anonymous connections are multiplexed over them. The sequence of mixes is strictly defined at connection start up for any anonymous connection.

There exist several implementations of the concepts described above. In the following, we will present the most important ones.

Tor Onion Routing (Tor)[970] is a second-generation implementation of the onion routing concept, "designed to anonymize TCP-based applications", using the SOCKS proxy.[971] Since most internet applications build upon TCP and support SOCKS, Tor can be used by these applications without modification. In Tor, multiple network connections share the same route of mixes in order to improve efficiency and anonymity; furthermore Tor introduces end-to-end integrity checking of the sent messages. Tor is heavily used in Germany: 45% of the network's total bandwidth is provided by German onion routers, while "Germany makes up 2,304 of the 7,571 total Tor clients, which is 30.4%".[972]

Java Anon Proxy (JAP) and the AN.ON service,[973] later renamed to JonDo and JonDonym and commercialised by Jondos GmbH,[974] provide means to anonymously connect to web services using fixed mix cascades. AN.ON uses a symmetric encryption scheme for inter-mix communication. Therefore each mix needs to agree on a symmetric key with both the previous and the next mix server in the mix cascade. AN.ON does not provide confidentiality of the messages, since only the headers of the network packets are encrypted. By using symmetric encryption and not providing confidentiality, AN.ON can provide anonymous web access with a relatively low cost factor.

The Invisible Internet Project (I2P)[975] is a fully distributed, autonomous message-oriented middleware ensuring confidential and anonymous communication within the I2P network. There exist outbound proxies that allow use of the normal web outside the I2P network, yet I2P can then ensure anonymity only. Existing applications may be integrated into the I2P network using SOCKS proxies. "Anonymity enabled applications" for several application domains have been developed within the project (e.g. web browsing, email, online chat, and file sharing), since nearly every legacy application "routinely exposes what, in an anonymous context, is sensitive information".

The goal of Freenet[976] is to provide a completely decentralized, uncensorable, scalable, highly-available, and fault-tolerant information storage while providing privacy for information producers. Freenet is designed to publish information by pooling the unused disk space of the network's participants. Privacy is maintained using Chaum mixes, making it impossible for participants to tell whether

968 Goldschlag/Reed/Syverson 1999.
969 Reed/Syverson/Goldschlag 1998.
970 Dingledine/Mathewson/Syverson 2004.
971 Leech/Ganis/Lee/Kuris/Koblas/Jones 1996.
972 McCoy/Bauer/Grunwald/Kohno/Sicker 2008.
973 Köpsell 2010.
974 http://anonymous-proxy-servers.net.
975 http://www.i2p2.de.
976 Clarke/Miller/Hong/Sandberg/Wiley 2002.

its predecessor was the originator of a message or merely forwarding it. Similarly, a sender of a message cannot tell whether the immediate receiver "is the true recipient or will continue forwarding it". Therefore, Freenet protects the provider, the consumer, and the holder of information.

Accountability Protocols

Andersen et al.[977] argue that today's network architectures (including the Internet) lack accountability because of the missing ability to associate actions with the responsible entities. Though the concept of accountability does not improve privacy per se, it may improve privacy by tying usage and sharing of data to entities.

Seneviratne and Kagal[978] motivate their proposal of an Accountable Hyper Text Transfer Protocol (HTTPA) with their belief that "users should be aware of and ideally in control of information about them on the web". In HTTPA, data provider and data consumer agree on restrictions for data usage and the intentions for data access before the actual data transfer. Additionally, both data provider and data consumer must identify themselves before the data transfer. Independent trusted provenance trackers log all information pertaining to a data transfer, including "the specified intent of access, and the agreed upon usage restrictions". If a data provider finds that someone else misused her data, a provenance trail can be produced with the help of the trusted provenance tracker.

According to Bender et al.[979], an accountability architecture should provide anonymity while telling users to what extent privacy is actually provided. Furthermore, servers would be able to identify, filter, and report repeat abusers. They therefore propose separating routing from accountability and introducing accountability as a network service. Sender and receiver of a message must then agree to use (and trust) the same accountability service. The accountability service acts as a certificate authority and provides clients with identifiers and public key certificates after they have proven their identity. Clients then digitally sign their messages and may use different identifiers to preserve anonymity. Upon misuse, the accountability service may reveal, according to its privacy policy, the identity of the sender.

Though accountability provides means to track the sharing and usage of data, it introduces privacy threats for the senders of messages and the need to trust a third party. Furthermore, it is worth discussing whether anonymity, privacy, and accountability can be maintained simultaneously.

4.4.4 INFRASTRUCTURE LEVEL

Secure Data Storage

The main purpose of secure data storage solutions such as (full) disc encryption[980] or memory encryption[981] is to bring confidentiality and integrity properties to the level of persistent (e.g. hard disc drives) or non-persistent (e.g. system memory) data storage. Because these security properties closely relate to privacy, (e.g. maintaining the confidentiality of private data records may help to prevent their unintended or impermissible usage), storage encryption techniques in many cases contribute to privacy-enhancing approaches. There exist a wide range of methods and approaches to secure the storage of data, differing in the types of data and storage media that can be protected, the security goals, and the way this protection is realized.

One of the most commonly used ones is the protection of persistent memory by encrypting complete storage devices or parts of it. Popular examples of this type of secure data

977 Andersen/Balakrishnan/Feamster/Koponen/Moon/Shenker 2008.
978 Seneviratne/Kagal 2011.
979 Bender/Spring/Levin/Bhattacharjee 2007.
980 Diesburg/Wang 2010.
981 Enck/Butler/Richardson/McDaniel/Smith 2008.

storage techniques are Microsoft's Bitlocker[982], TrueCrypt[983], or Apple's FileVault[984]. All these solutions share the common goal to provide full disk encryption, in contrast to solutions like the eCryptfs Linux project[985] that incorporate cryptographic functions directly into the file system drivers. Yet, only securing the persistent storage does not entirely solve the secure data storage problem, as data normally must be decrypted at system runtime upon use and thus is unprotected in the main memory of the system. Recent experiments showed that this unprotected memory is prone to attacks that result in a disclosure of the plain memory content.[986] Therefore memory encryption solutions like CryptKeeper[987] or CryptoPage[988] focus on the protection of the non-persistent memory of a system by applying cryptographic function on the memory write and read operations.

Trusted Computing

The concept of Trusted Computing is based on the desire to establish trust in that a system consistently behaves in a specified way, by verifying the integrity of the corresponding (hardware and software) infrastructure.[989]

To reach this goal, a special sealed hardware component, the Trusted Platform Module (TPM), which encloses a cryptographic key, is introduced. This component is secured against being read by any other component of the system. In addition, the TPM is, among others, also capable of generating pseudo-random numbers, as well as providing secure storage for additional cryptographic keys or hash values.[990]

Please note that the TPM itself is a passive device and only acts as a secure basis for further security mechanisms such as integrity checks or secure key generation.

The most popular Trusted Computing specification at the time of writing is standardized by the Trusted Computing Group (TCG), the successor organization of the Trusted Computing Platform Alliance (TCPA) and consists of the following basic principles:

- **Memory Curtaining** describes the approach to protect the system memory in a way that securely isolates parts that contain sensitive information from non-sensitive memory parts. By this, sensitive information such as cryptographic keys can be effectively protected from being read or modified by non-authorized software. Not even the operating system itself has full access to sensitive memory parts, thus this approach also protects sensitive data even if the operating system has been compromised. One popular implementation for this concept is Intel's Trusted Execution Technology (TXT).
- **Sealed Storage** refers to the concept of binding the usage of data to a particular hardware and software configuration. This means that Trusted Computing allows the specification of a particular set of data to only be accessible and usable by one particular system. Microsoft's Bitlocker implements this concept and, for example, only allows access to a hard drive if it is attached to one particular system.
- **Remote Attestation** means the remote verification of the integrity of a system or the detection of changes to important system properties by an authorized external entity. This basically works by the tamper-proof, TPM-based generation of certificates that represent the current configuration of a system. By comparing these certificates with default values that represent the intended system state, the external entity can check whether the

982 http://technet.microsoft.com/en-us/library/cc766200(WS.10).aspx.
983 http://www.truecrypt.org/docs/.
984 http://support.apple.com/kb/HT4790.
985 https://launchpad.net/ecryptfs/.
986 Halderman/Schoen/Heninger/Clarkson/Paul/Calandrino/Feldman/Appelbaum/Felten 2009.
987 Peterson 2010.
988 Duc/Keryell 2006.
989 Rosteck 2008.
990 http://www.trustedcomputinggroup.org/resources/tpm_main_specification.

system's state corresponds to the intended state. As the certificates are signed using a unique private key within the TPM, this procedure is considered privacy-intrusive, as the usage of the private key in theory allows one to uniquely identify the system the certificate belongs to.

- **Direct Anonymous Attestation (DAA)** is the privacy-preserving, zero-knowledge proof-based alternative to remote attestation. DAA works by letting the TPM choose a secret message that is signed by an external attester, which then is used to anonymously proof the attestation to the verifying party due to the knowledge about the signature of the secret message.
- **Trusted Software Stack (TSS)** is the defined software interface to access the functionalities of the TPM. It is the only way for a software artefact to communicate with the TPM. The reason for restricting the communication with the TPM to the usage of the TSS is to encapsulate all security-critical functionality within a standardized framework. This encapsulation prevents wrongful usage attempts and increases overall security by reducing the chance of failures due to buggy implementations.

By exploiting all or parts of these concepts, Trusted Computing can ensure that a system behaves according to a predefined manner by establishing a so-called Chain of Trust for the boot process. This means that the integrity of the system's components involved in the boot procedure (starting with the BIOS and going up to the operating system) is checked before control is handed over to them. For example, first the BIOS code is hashed, the hash is securely stored within the TPM, and only after that the control is handed to the BIOS. This step is repeated for all remaining parts of the boot sequence, always extending the hash value of the previous boot step. Eventually, the resulting hash value can be compared against a set of reference values to ensure that no unwanted modifications happen to the components of the boot procedure. As the TPM is assumed to be tamper-proof and thus secure, the TPM is the root of trust for this integrity verification procedure.

This integrity verification of the boot process is only one application of Trusted Computing concepts, which are also used for purposes of Digital Rights Management, secure drive encryption, or trusted virtualization.[991]

While Trusted Computing offers a number of valuable contributions to establish trust in the integrity of a system and to allow sophisticated security mechanisms, it is also a broad point of criticism. These include privacy concerns, potential burdens for the development of free software, and the generated monopolistic status of a small number of hardware and software vendors.[992]

4.4.5 COMBINED AND INTEGRATED SOLUTIONS

After having described theoretical concepts and isolated technical techniques to tackle the problem of internet privacy, this section gives on overview of solutions which integrate these concepts.

PRIME

The goal of the PRIME EU Project was to demonstrate the viability of a privacy-enhancing identity management system that puts individuals in control of their personal data.[993] PRIME integrates several concepts and techniques described in this report by providing a middleware that can and must be leveraged by applications both on the server side and the client side. The prototype supports, among others, (semi-) automatic privacy policy negotiations, anonymous and pseudonymous interactions, enforcement of machine-readable privacy-policies, private credentials, and anonymous communication channels using Tor. However, the trustworthiness of the PRIME components is out of the scope of the project's

991 Löhr/Ramasamy/Sadeghi/Schulz/Schunter/Stüble 2007.
992 Yung 2003.
993 Leenes/Schallaböck/Hansen 2008.

work and must therefore be "maximised by technical means (e.g. cryptographic techniques) and non-technical means (e.g. certification and assurance)".

Privacy Enhancing Linux Distributions

In recent years several Privacy Enhancing Linux Distributions (PELD) have been developed. The Polippix[994] project is maintained by the IT-Political Association of Denmark and its objective "is to protect users against all violations of online privacy".[995] The goal of Tails[996] is to provide a software solution that allows for the usage of popular Internet technologies while maintaining the user's privacy, in particular with respect to anonymity. Liberté Linux'[997] primary purpose is to enable "anyone to communicate safely and covertly in hostile environments".

All of these solutions try to reach their goal by providing a secured and hardened live Linux Operating System by integrating, among others, well-known mechanisms for secure storage and secure, anonymous, and traceless networking. Such mechanisms include anonymous networking techniques like Tor, I2P, and Privoxy, as well as applications or application extensions like Vidalia (a graphical controller for Tor)[998], Tor Browser Bundle, Tor IM (Instant Messaging) Bundle[999], HTTPS Everywhere[1000], and OpenPGP[1001,1002] for email.

4.4.6 PROVISIONAL CONCLUSION

In this report, we have described several concepts and techniques that are directed toward the improvement of privacy on the internet and have structured them similarly to the ISO/OSI reference model. It seems that a plethora of privacy-enhancing concepts and mechanisms exist at each layer, providing a wide spectrum of options to maintain privacy.

However, protecting privacy using only one technique is insufficient, since "the security of a computer system or network is a function of many factors [and] defects in OS security, poor quality of random number sources, sloppy system management protocols and practices, etc., can all degrade the security".[1003] In order to maintain privacy, different mechanisms from several layers must be used and integrated, hence providing an overarching solution protecting privacy at all layers. However, such integrating solutions are lacking.

The PRIME project and privacy enhancing Linux distributions take steps in the correct direction, yet many problems are still pending. These problems include

- user-friendly und user-understandable privacy interfaces that make privacy frameworks usable for end users,
- mechanisms that allow users to exercise at least some control over their data once it has been released to other parties, and
- server-side mechanisms that aim at protecting privacy by going beyond regular (e.g. annual) privacy audits and assisting system users and administrators.

It also needs to be mentioned, that many technical solutions that aim (directly or indirectly) to increase the level of privacy on the internet, or try to tackle common threats to

994 http://www.polippix.org/.
995 Larsen 2008.
996 https://tails.boum.org/.
997 http://www.dee.su/liberte.
998 https://www.torproject.org/projects/vidalia.html.en.
999 https://www.torproject.org/projects/torbrowser.html.en.
1000 https://www.eff.org/https-everywhere.
1001 http://www.openpgp.org/.
1002 Callas/Donnerhacke/Finney/Shaw/Thayer 2007.
1003 Kent/Seo 2005.

privacy, introduce new threats to privacy themselves. Many solutions that rely on public key cryptography, for example, often suffer from the necessity of a public key infrastructure. For example, the usage of TLS/SSL depends on digital certificates that, in order to be verifiable, must be issued by some external trusted third party. As this trusted third party maintains the connection between all involved parties and their digital certificates, this third party is capable of significantly degrading privacy, for example if it is compromised. Other examples for this problem are anonymization Proxies which offer the user the possibility of some level of anonymity with respect to the activities performed through the proxy. Concurrently, the proxy itself somehow threatens privacy, as it knows the links between the anonymized actions and the respective proxy clients.

In summary, the usage of privacy-enhancing tools in many cases induces additional security and privacy risks, or even worse, reduces the overall level of privacy. As there rarely exist combined and integrated solutions that use privacy-enhancing technology in a coherent and generic way, the application of the single privacy-enhancing technologies has to be carefully and individually considered with respect to the concrete situation and system setting.

4.5 CONCLUSION

We all benefit from the emerging advances in electronic society. Such technologies, however, put our data and privacy at higher risks. Therefore, investigating privacy on the Internet is becoming more crucial than ever.

We presented the state of Internet privacy from a technical perspective. We began by investigating some privacy-invasive scenarios on the Internet. On the basis of these examined scenarios we reviewed the technical privacy-threatening risks and corresponding existing solutions. Privacy threats arise from data collection, aggregation, and storage when the data is not protected and used appropriately. We explored numerous technical solutions for privacy protection. However, many of them are not yet widely used. Their usefulness (including usability) is still to be established in the applicable legal, social, ethical, and economic contexts.

LITERATURE

AbuHmed/Mohaisen/Nyang 2008
AbuHmed, Tamer/Mohaisen, Abedelaziz/Nyang, DaeHun: *Magazine of Korea Telecommunication Society*, Vol. 24, No. 11: 25–36, 2007.

acatech 2011
acatech (Hrsg.): *Cyber-Physical Systems – Innovationsmotor für Mobilität, Gesundheit, Energie und Produktion* (acatech POSITION), Heidelberg u.a.: Springer Verlag 2011. http://www.acatech.de/fileadmin/user_upload/Baumstruktur_nach_Website/Acatech/root/de/Publikationen/Stellungnahmen/POSITION_CPS_NEU_WEB_120130_final.pdf

Acquisti/Gross/Stutzman 2011
Acquisti, Alessandro/Gross, Ralph/Stutzman, Fred: *Face Recognition Study*, 2011. URL: http://www.heinz.cmu.edu/~acquisti/face-recognition-study-FAQ/

Acquisti/Gross 2009
Acquisti, Alessandro/Gross, Ralph: *Predicting Social Security Numbers from Public Data*, 106 PROC. NAT'L, ACAD, SCI. 10975-80, 2009.

Abdul-Rahman 1997
Abdul-Rahman, Alfarez: *The pgp trust model*, EDI-Forum, the Journal of Electronic: 1–6. 1997.

Albanesius 2012
Albanesius, Chloe: *Web Surfing Activity Vulnerable to 'History Sniffing'*, Report Says. PCMAC, 2010.

Alsaid/Martin 2002
Alsaid, Adil/Martin, David: *Detecting web bugs with Bugnosis: Privacy advocacy through education*, Proceedings of Workshop on Privacy Enhancing Technologies, Springer-Verlag, 2002.

Andersen/Balakrishnan/Feamster/Koponen/Moon/Shenker 2008
Andersen, David G./Balakrishnan, Hari/Feamster, Nick/Koponen, Teemu/Moon, Daekyeong/Shenker, Scott: *Accountable Internet Protocol (AIP)*, Proceedings of the ACM SIGCOMM conference on Data communication SIGCOMM 08 38 (4): 339–350, 2008.

Anderson/Brusa/Price/Jerell/Jo 2011
Anderson, Matt/Brusa, Jennifer/Price, Jerell/ Sims, Jo: *Turning "Like" to "Buy": Social Media Emerges as a Commerce Channel*, 2011. URL: http://www.booz.com/global/home/what_we_think/reports_and_white_papers/ic-display/49009342; http://www.booz.com/media/uploads/BaC-Turning_Like_to_Buy.pdf

Anderson/Fuloria 2010
Anderson, Ross/Fuloria, Shailendra: *Who controls the off switch?*, First IEEE International Conference Smart Grid Communications (SmartGridComm): 96–101, 2010. URL: http://www.cl.cam.ac.uk/~rja14/Papers/meters-offswitch.pdf

Ansari/Rajeev/Chandrashekar 2002/2003
Ansari, Sabeel/Rajeev, S. G./Chandrashekar, H. S.: *Packet sniffing: a brief introduction*, Potentials, IEEE , Vol. 21, No. 5: 17–19, Dec 2002/Jan 2003.

Arshad 2004
Arshad, Fahd: *Privacy Fox – A JavaScript-based P3P Agent for Mozilla Firefox*, 2004.

Adolphs/Winkelmann 2010
Adolphs, Christoph/Winkelmann, Axel: *A rigorous literature review on personalization research in e-commerce* (2000–2008), In Journal of Electronic Commerce Research, Vol. 11:326–341, 2010.

Adomavicius/Tuzhilin 2005
Adomavicius, Gediminas/Tuzhilin, Alexander: *Toward the next generation of recommender systems: a survey of the state-of-the-art and possible extensions*, Knowledge and Data Engineering, IEEE, Vol. 17, No. 6: 734–749, 2005.

Badrul/Karypis/Konstan/Riedl 2000
Sarwar, Badrul/Karypis, George/Konstan, Joseph/Riedl, John: *Analysis of Recommendation Algorithms for E-Commerce*, Proceedings of the 2nd ACM conference on Electronic commerce (EC ,00):158–167, 2000.

Baker/Shah/Rosenthal/Roussopoulos/Maniatis/Giuli/Bungale 2006
Baker, Mary/Shah, Mehul/Rosenthal, David S. H./Roussopoulos, Mema/Maniatis, Petros/Giuli, TJ/Bungale, Prashanth: *A Fresh Look at the Reliability of Long-term Digital Storage*, Proceedings of Computer systems (EuroSys): 221–234, 2006.

Barbaro/Zeller 2006
Barbaro, Michael/Zeller, Tom Jr.: *A Face Is Exposed for AOL Searcher No. 4417749*, The New York Times, 09/08/2006. URL: http://www.nytimes.com/2006/08/09/technology/09aol.html?pagewanted=all

Bender/Spring/Levin/Bhattacharjee 2007
Bender, Adam/Spring, Neil/Levin, Dave/Bhattacharjee, Bobby: *Accountability as a service*, Proceedings of the 3rd USENIX workshop on Steps to reducing unwanted traffic on the internet, USENIX Association, Article 5, 2007.

Bermann 2006
Bermann, S.: *Privacy and Access to Public Records in the Information Age*, Bepress Legal Series, page 1303, 2006.

Besmer/Watson/Lipford 2010
Besmer, Andrew/Watson, Jason/Lipford, Heather Richter: *The Impact of Social Navigation on Privacy Policy Configuration*, Proceedings of the Sixth Symposium on Usable Privacy and Security (SOUPS 2010), 2010.

Bittau/Hamburg/Handley/Mazieres/Boneh 2010
Bittau, Andrea/Hamburg, Michael/Handley, Mark/Mazieres, David/Boneh, Dan: *The case for ubiquitous transport-level encryption*, Proceedings of the 19th USENIX conference on Security, 2010.

Bollier 2010
Bollier, D.: *The Promise and Peril of Big Data*, Program: 1–66, 2010. URL: http://www.aspeninstitute.org/sites/default/files/content/docs/pubs/InfoTech09.pdf

Boutin 2006
Boutin, Paul: *You Are What You Search – AOL's data leak reveals the seven ways people search the Web*, 2006. URL: http://www.slate.com/articles/technology/technology/2006/08/you_are_what_you_search.html

boyd/Ellison2007
boyd, danah M./ Ellison, Nicole: *Social network sites: Definition, history, and scholarship*, Journal of Computer-Mediated Communication, Vol. 13, No. 1: 210–230, 2007.

boyd/Crawford 2011
boyd, d, Crawford, K.: *Six Provocations for Big Data*, Computer: 1–17, 2011. URL: http://ssrn.com/paper=1926431.

Bradley 2012
Bradley, Tony: *Introduction to Packet Sniffing*. URL: http://netsecurity.about.com/cs/hackertools/a/aa121403.htm/ [12/1/2012].

Breese/Heckerman/Kadie 1998
Breese, J. S., Heckerman, D., and Kadie, C.: *Empirical analysis of predictive algorithms for collaborative filtering*, Proceedings of the Fourteenth Conference on University in Artificial Intelligence, Madison, WI, 1998.

Brueckner/Voss 2005
Brueckner, Lars/Voss, Marco: *MozPETs – a privacy enhanced Web Browser*, Conference on Privacy, Security and Trust, 2005.

BSI 2011
Federal Office for Information Security (BSI): *White Paper Security Recommendations for Cloud Computing Providers (Minimum information security requirements)*, 22/06/2011. URL: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Minimum_information/SecurityRecommendationsCloudComputingProviders.pdf?__blob=publicationFile

Buchegger/Schiöberg/Vu/Datta 2009
S. Buchegger/D. Schiöberg/L. H. Vu/A. Datta: *PeerSoN: P2P Social Networking – Early Experiences and Insights*, Proceedings of the Second ACM Workshop on Social Network Systems Social Network Systems, 2009.

Buchmann/May/Vollmer 2006
Buchmann, Johannes /May, Alexander/ Vollmer, Ulrich: *Perspectives for cryptographic long-term security*, Commun. ACM, Vol. 49, Issue 9: 50–55, 2006.

Calandrino/Kilzer/Narayanan/Felten/Shmatikov 2011
Calandrino, Joseph A./Kilzer, Ann/Narayanan, Arvind/ Felten, Edward W./Shmatikov, Vitaly: "*You Might Also Like: " Privacy Risks of Collaborative Filtering*, Proceedings of the IEEE Symposium on Security and Privacy (SP '11), 2011.

Callas/Donnerhacke/Finney/Shaw/Thayer 2007
Callas, J./Donnerhacke, L./Finney, H./Shaw, D./Thayer, R.: *RFC 4880: OpenPGP Message Format*, The Internet Engineering Task Force, 2007.

Canetti 2004
Canetti, Ran: *Universally Composable Signature, Certification, and Authentication*, Proceedings of the 17th IEEE workshop on Computer Security Foundations: 219–233, IEEE Computer Society, Washington, DC, USA, 2004.

Carneiro/Mylonakis 2009
Carneiro, Herman Anthony/ Mylonakis, Eleftherios: *Google Trends: A Web-Based Tool for Real-Time Surveillance of Disease Outbreaks*, 2009/11/15. URL: http://cid.oxfordjournals.org/content/49/10/1557.abstract

Cashmore 2010
Cashmore, P.: *Should Facebook add a dislike button?*, CNN.com, 22/07/2010. URL:http://edition.cnn.com/2010/TECH/social.media/07/22/facebook.dislike.cashmore/

Castelluccia 2012
Castelluccia, Claude: *Behavioural Tracking on the Internet: A Technical Perspective*, book chapter of European Data Protection: In Good Health?, Springer Netherlands, 2012.

Castelluccia/Cristofaro/Perito 2010
Castelluccia, Claude/ De Cristofaro, Emiliano/Perito, Daniele: *Private Information Disclosure from Web Searches*, PETS'10 Proceedings of the 10th international conference on Privacy enhancing technologies Springer-Verlag Berlin, 2010.

Castellucia/Druschel/Fischer Hübner/Pasic/Preneel/ Tschofenig 2010
Castellucia, Claude/Druschel, Peter/Fischer Hübner, Simone/Pasic, Aljosa/Preneel, Bart /Tschofenig, Hannes: *Privacy, Accountability and Trust – Challenges and Opportunities*, European Network and information Security Agency (ENISA), 2010.

Caviglione/Coccoli 2011
Caviglione, L./Coccoli, M.: *Privacy problems with Web 2.0*, Computer Fraud Security: 19–16, 2011.

Chaum 1981
Chaum, David L.: *Untraceable electronic mail, return addresses, and digital pseudonyms*, Communications of the ACM, Vol. 24 Issue 2: 84–90, 1981.

Chapple 2011
Chapple, Mike: *Data Mining: An Introduction.* URL: http://databases.about.com/od/datamining/a/datamining.htm/ [11/12/2011].

Chellappa/Sin 2005
Chellappa, Ramnath K./Sin, Raymond G.: *Personalization versus Privacy: An Empirical Examination of the Online Consumer's Dilemma*, Inf. Technol. and Management, Vol. 6: 181–202, 2005.

Chen/Rahman 2008
G. Chen and F. Rahman. Analysing Privacy Designs of Mobile Social Networking Applications, Proc. Int'l. Symp. Trust, Security and Privacy for Pervasive Applications, 2008.

Clarke/Miller/Hong/Sandberg/Wiley 2002
Clarke, Ian/Miller, Scott G./Hong, Theodore W./Sandberg Oskar/Wiley, Brandon: *Protecting Free Expression Online with Freenet*. In: IEEE Internet Computing, Vol. 6 Issue 1: 40–49, 2002.

Clauss/Koehntopp 2001
Clauss, Sebastian/Koehntopp, Marit: *Identity management and its support of multilateral security*, Computer Networks, Vol. 37, Issue 2: 205–219, 2001.

Clifton 2008
Clifton, Brian: *Web Analiytics- Web Traffic Data Sources & Vendor Comparison*, White paper in conjunction with Omega Digital Media Ltd, 2008.

Computerwoche 2011
Cloer, Thomas: *E-Commerce wird mobiler und sozialer*, Computerwoche, 20/10/2011. URL:http://www.computerwoche.de/netzwerke/web/2498237/

Constantin 2011
Constantin, Lucian: *Facebook Spam Worm Propagates via Persistent XSS Vulnerability*, Softpedia, 10/03/2011. URL http://news.softpedia.com/news/Facebook-Spam-Worm-Propagates-via-Persistent-XSS-Vulnerability-188934.shtml/ [23/05/2012].

Cranor/Arjula/Guduru 2002
Cranor, Lorrie Faith/Arjula, Manjula/Guduru, Praveen: *Use of a P3P user agent by early adopters*, Proceedings of the 2002 ACM workshop on Privacy in the Electronic Society: 1–10, ACM, 2002.

Cranor 2003
Cranor, Lorrie Faith: *I didn't buy it for myself' privacy and ecommerce personalization*, In *Proceedings of ACM workshop on Privacy in the electronic society* (WPES 03):111–117, 2003.

Cranor/McDonald/Egelman/Sheng 2007
Cranor, Lorrie Faith/McDonald, Aleecia M./Egelman, Serge/Sheng, Steve: *Privacy Policy Trends Report*, CyLab Privacy Interest Group, 2007.

CRR 2011
Center for Retail Research: *Online Retailing: Britain and Europe 2012*, 2012. URL: http://www.retailresearch.org/onlineretailing.php, [30/01/2012]

CSA 2009
Cloud Security Alliance: *Security Guidance for Critical Areas of Focus in Cloud Computing V2.1*, 12/2009. URL: http://www.cloudsecurityalliance.org/csaguide.pdf

CSA 2010
Cloud Security Alliance: *Top Threats to Cloud Computing*, 03/2010. URL:http://www.cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf

Cutillo/Molva/Strufe 2009
Cutillo, Leucio/Molva, Refik/Strufe, Thorsten: *Safebook: A privacy-preserving online social network leveraging on real-life trust*, IEEE Communications Magazine, Vol. 47,: 94–101, 2009.

Cubrilovic 2011
Cubrilovic, Nik: URL: https://plus.google.com/105854725972317368943/posts/ [30/05/2012].

Daemen/Rijmen 2002
Daemen, Joan/Rijmen, Vincent: *The Design of Rijndael: AES – The Advanced Encryption Standard*, Springer-Verlag New York, Inc., Secaucus, 2002.

Daly 2010
Daly, Angela: *The Legality of Deep Packet Inspection*, 2010. URL: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1628024.

David/Zwerdling/Guy/Ofek-Koifman/Har'el/Ronen/Uziel/Yogev/Chernov 2009
Carmel, David/Zwerdling, Naama/Guy, Ido/Ofek-Koifman, Shila/Har'el, Nadav/Ronen, Inbal/Uziel, Erel/Yogev, Sivan/Chernov, Sergey: *Personalized social search based on the user's social network*, Proceedings of the 18th ACM conference on Information and knowledge management (CIKM ,09): 1227–1236, ACM, 2009.

Davison/Maraist/Bing 2011
Davison, H. K./Maraist, C./Bing, M. N.: *Friend or Foe? The Promise and Pitfalls of Using Social Networking Sites for HR Decisions*, Journal of Business and Psychology, Vol. 26, Issue: 2: 153–159, 2011.

Davos 2012
The World Economic Forum: *Big Data, Big Impact: New Possibilities for International Development*, 2012. URL: http://www.weforum.org/reports/big-data-big-impact-new-possibilitiesinternational-development

Deloitte 2011
Deloitte: *Social network advertising: how big can it get?*, 2011. URL: http://www.deloitte.com/view/en_GX/global/industries/technology-media-telecommunications/tmt-predictions-2011/media-2011/eab5bcd1ed47d210VgnVCM2000001b56f00aRCRD.htm, [Last visited 30/01/2012].

Dierks/Rescorla 2008
Dierks, Tim/Rescorla, Eric: RFC 5246: *The Transport Layer Security (TLS) Protocol Version 1.2*. IETF., The Internet Engineering Task Force, 2008.

Diesburg/Wang 2010
Diesburg, Sarah M./Wang, An-I Andy: *A survey of confidential data storage and deletion methods*, ACM Computing Surveys, Vol. 43 Issue 1, Article No. 2, 2010.

Dingledine/Mathewson/Syverson 2004
Dingledine, Roger/Mathewson, Nick/Syverson Paul: Tor: *The second-generation onion router*, Proceedings of the 13th conference on USENIX Security Symposium, Vol. 13: 303–320, 2004.

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.

Dobias 2011
Dobias, Jaromir: *Privacy Effects of Web Bugs Amplified by Web 2.0*, Book Chapter of Privacy and Identity Management for Life, Springer Boston, 2011.

Douceur 2002
Douceur, John R: *The Sybil Attack*, International Workshop on Peer-To-Peer Systems, Lecture Notes in Computer Science, Vol. 2429: 251–260, Springer Berlin/Heidelberg, 2002.

Duc/Keryell 2006
Duc, Guillaume/Keryell, Ronan: CryptoPage: *An Efficient Secure Architecture with Memory Encryption, Integrity and Information Leakage Protection*, Computer Security Applications Conference: 483–492, 2006.

Dumitru 2009
Dumitru, Bogdan: *The Risks of Social Networking and the Corporate Network*, 2009. URL: http://www.itbusinessedge.com/cm/community/features/guestopinions/blog/the-risks-of-social-networking-and-the-corporate-network/?cs=33877

Dwork 2008
Dwork, Cynthia: *Differential Privacy: A Survey of Results*, Theory and Applications of Models of Computation, Lecture Notes in Computer Science Vol. 4978: 1–19, Springer Berlin/Heidelberg, 2008.

Dwork/Smith 2009
Dwork, Cynthia/Smith, Adam: *Differential Privacy for Statistics*: What we Know and What we Want to Learn, Journal of Privacy and Confidentiality, Vol. 1 Issue 2: 135–154, 2009.

Eckersley 2010
Eckersley, Peter: *How Unique Is Your Web Browser?*, Privacy Enhancing Technologies: 1–18, 2010.

Edelman 2009
Edelman, Benjamin: *Adverse selection in online "trust" certifications*, Proceedings of the 11th International Conference on Electronic Commerce: 205–212, ACM New York, 2009.

Edwards/Riley 2011.
Edwards, Cliff/Riley, Michael: *Sony Data Breach Exposes Users to Years of Identity-Theft Risk. Bloomberg*, 03/05/2011. URL: http://www.bloomberg.com/news/2011-05-03/sony-breach-exposes-users-to-identity-theft-as-credit-card-threat-recedes.html

Egele/Moser/Kruegel/Kirda 2011
Egele, Manuel/Moser, Andreas/Kruegel, Christopher/Kirda, Engin: *PoX: Protecting users from malicious Facebook applications*, IEEE PERCOM Workshops, 2011.

Eirinaki/Vazirgiannis 2003
Eirinaki, Magdalini/Vazirgiannis, Michalis: *Web mining for web personalization, ACM Trans. Internet Technol.* 3, 1: 1–27, 2003.

ElGamal 1985
El Gamal, Taher: *A public key cryptosystem and a signature scheme based on discrete logarithms*, Proceedings of CRYPTO 84 on Advances in cryptology: 10–18, Springer-Verlag New York, Inc., 1985.

E-Marketer 2011
E-Marketer: *US M-Commerce Sales to Grow 91% to $6.7 Billion in 2011*, 01/12/2011. URL:http://www.emarketer.com/PressRelease.aspx?R=1008716

Enck/Butler/Richardson/McDaniel/Smith 2008
Enck, William/Butler, Kevin/Richardson, Thomas/McDaniel, Patrick/Smith, Adam: *Defending Against Attacks on Main Memory Persistence*, Proceedings of the 2008 Annual Computer Security Applications Conference: 65–74, IEEE Computer Society, 2008.

Enev/Gupta/Kohno/Patel 2011
Enev, Miro /Gupta, Sidhant /Kohno, Tadayoshi/Patel, Shwetak: T*elevisions, Video Privacy, and Powerline Electromagnetic Interference*, http://abstract.cs.washington.edu/~miro/docs/ccs2011.pdf

ENISA 2007
ENISA: Security Issues and Recommendations for Online Social Networks, Position Paper,11/2007. URL:http://fredstutzman.com/papers/ENISA2007.pdf

ENISA 2009
ENISA: Cloud Computing Risk Assessment, 2009. URL: http://www.enisa.europa.eu/activities/risk-management/files/deliverables/cloud-computing-information-assurance-framework/at_download/fullReport

EPIC on Re-identification
Re-identification. URL: http://epic.org/privacy/reidentification/ [23/05/2012].

Del Sesto/Frankel 2008
Del Sesto, Ronald W. Jr./Frankel, Jon: How deep Packet Inspection changed the Privacy debate, Bingham (Law Firm), 2008. URL: http://www.bingham.com/Publications/Files/2008/09/How-Deep-Packet-Inspection-Changed-the-Privacy-Debate /[30/5/2012].

Facebook 2010
Facebook: *The Value of a Liker by Facebook + Media*, 29/09/2010. URL: http://www.facebook.com/notes/facebook-media/value-of-a-liker/150630338305797

Fletcher 2010
Fletcher, Dan: *How Facebook Is Redefining Privacy*, Time Magazine, 20/05/2010. URL: http://www.time.com/time/magazine/article/0,9171,1990798,00.html#ixzz1lpfqrijz

FTC 2000
Federal Trade Commission: *Online Profiling: A Report to Congress-Part 2-Recommendations*, 2000.

FTC 2009
Federal Trade Commission, *FTC Staff Report: Self-Regulatory Principles For Online Behavioral Advertising-Behavioral Advertising Tracking, Targeting, & Technology*, 02/2009. URL: http://www.ftc.gov/os/2009/02/P085400behavadreport.pdf

FTC 2010
Federal Trade Commission: *Protecting Consumer Privacy in an Era of Rapid Change*, 2010. URL: http://www.ftc.gov// [23/05/2012].

Freudiger/Shokri/Hubaux 2011
Freudiger,J./Shokri,R./Hubaux, J.-P.: *Evaluating the Privacy Risk of Location-Based Services*, Financial Cryptography and Data Security (FC), 2011.

Friedland/Sommer 2010
Friedland, G./Sommer, R. : Cybercasing the joint: *On the privacy implications of geo-tagging*, USENIX Workshop on Hot Topics in Security, 2010.

Gartner 2009
Shen et al. : *Dataquest Insight: The Top 10 Consumer Mobile Applications in 2012*, Gartner Research, 2009.

Gartner 2010
Gartner, Inc.: *Forecast: Public Cloud Services, Worldwide and Regions*, Industry Sectors, 2009–2014. 02/6/2010. URL: http://www.gartner.com/resId=1378513

Gerck 2002
Gerck, Ed.: *Trust as Qualified Reliance on Information Trust as Qualified*, Reading: 1071-6327, 2002. URL: http://nma.com/papers/it-trust-part1.pdf

Geyer/Freyne/Mobasher/Anand/Dugan 2010
Geyer, Werner/Freyne, Jill/Mobasher, Bamshad/Anand, Sarabjot Singh/Dugan, Casey: *Recommender Systems and the Social Web*, 2nd workshop on recommender systems and the social web, Proceedings of the fourth ACM conference on Recommender systems (RecSys ,10): 379–380, ACM, 2010.

Ginsberg/Mohebbi/Patel/Brammer/Smolinski/Brilliant 2009
Ginsberg, Jeremy/Mohebbi, Matthew H./Patel, Rajan S./Brammer, Lynnette/Smolinski, Mark S./Brilliant, Larry: *Detecting influenza epidemics using search engine query data*, Nature, Vol. 457, Macmillan Publishers, 2009.

Goldschlag/Reed/Syverson 1999
Goldschlag, David/Reed, Michael/Syverson, Paul: *Onion routing*, Communications of the ACM, Vol. 42 Issue 2: 39–41, 1999.

Google Reader 2012
Beware! *Google Reader Notifier for Firefox Is Now Crapwared*. URL: http://www.howtogeek.com/howto/2585/beware-google-reader-notifierfor-firefox-is-now-crapware/ [30/05/2012].

Goy/Ardissono/Petrone 2007
Goy, Anna/ Ardissono, Liliana/Petrone, Giovanna: *Personalization in e-commerce applications*. In the adaptive web, Peter Brusilovsky, Alfred Kobsa, and Wolfgang Nejdl (Eds.), Lecture Notes In Computer Science, Vol. 4321, Springer-Verlag, 2007.

Götz/Machanavajjhala/Wang/Xiao/Gehrke 2012
Gotz, Michaela/Machanavajjhala, Ashwin/Wang, Guozhang/Xiao, Xiaokui/Gehrke, Johannes: *Publishing Search Logs – A Comparative Study of Privacy Guarantees, IEEE Trans. On Knowl. and Data Eng.* Vol. 24:520-532, 2012.

Grance/Jansen 2011
Grance, T./Jansen, W.: *Guidelines on Security and Privacy in Public Cloud Computing*, NIST, NIST SP - 800-144, 2011. URL: http://www.nist.gov/manuscript-publication-search.cfm?pub_id=909494

Grandison/Sloman 2000
Grandison, Tyrone/Sloman, Morris: *A survey of trust in internet applications*, IEEE Communications Surveys & Tutorials, Vol. 3 No. 4: 2–16, 2000.

Griffiths 2010
Griffiths, Sarah: *Mobile social networking apps spark privacy concerns*, Hexus, 2010. URL: http://hexus.net/business/news/internet/25288-mobile-social-networkingapps-spark-privacy-concerns// [23.05.2012].

Gross/Acquisti 2005
Gross, R./Acquisti, A.: *Privacy and Information Revelation in Online Social Networks*, ACM Workshop on Privacy in the Electronic Society: 71–80, 2005.

Guarda/Zannone 2009
Guarda, P./Zannone, N.: *Towards the development of privacy-aware systems,* Inf. Softw. Technol., Vol. 51: 337–350, 2009.

Hagen/Manning/Souza 1999
Hagen, P. R./Manning, H./Souza, R.: Smart personalization, Technical report, Forrester Research, Cambridge, MA, 1999.

Halderman/Schoen/Heninger/Clarkson/Paul/Calandrino/Feldman/Appelbaum/Felten 2009
Halderman, J. Alex/Schoen, Seth D./Heninger, Nadia/Clarkson, William/Paul, William/Calandrino, Joseph A./Feldman, Ariel J./Appelbaum, Jacob/Felten, Edward W.: *Lest we remember: cold-boot attacks on encryption keys,* Communications of the ACM, Vol. 52 Issue 5: 91–98., 2009.

Hansen/Schwartz/Cooper 2008
Hansen, Marit/Schwartz, Ari/Cooper, Alissa: *Privacy and Identity Management*, IEEE Security & Privacy, Vol. 6 No. 2: 38–45, 2008.

Hansen 2008
Hansen, Marit/Pfitzmann, Andreas/Steinbrecher, Sandra: *Identity management throughout one's whole life*, Inf. Secur. Tech., Vol. 13, No. 2: 83–94, 2008.

Hansen 2009
Hansen, Marit: *Putting Privacy Pictograms into Practice – a European Perspective*, GI Jahrestagung 2009, 2009

Head/Yuan 2001
Head, Milena/ Yuan, Yufei: *Privacy Protection in Electronic Commerce*: A Theoretical Framework, Human Systems Management, 20: 149–160, 2001.

Hedbom 2009
Hedbom, Hans: *A Survey on Transparency Tools for Enhancing Privacy.* In: The Future of Identity in the Information Society, Springer, Vol. 298: 67–82, 2009.

Heuston 2011
Heuston, George Z.: *Privacy concerns: From social media aggregation to aggravation*. URL: http://www.oregonlive.com/argus/index.ssf/2011/01/privacy_concerns_from_social_m.html/[03/02/2012].

Hilty/Pretschner/Basin/Schaefer 2007
Hilty, Manuel/Pretschner, Alexander/Basin, David/ Schaefer, Christian/Walter, Thomas: *Monitors for usage control.* In: Trust Management, Springer, Vol. 238: 411–414, 2007.

Hill 2011
Hill, Kashmir: *Mark Zuckerberg's private photos exposed due to Facebook flaw*, Forbes, 12/06/2011. URL: http://www.forbes.com/sites/kashmirhill/2011/12/06/mark-zuckerbergs-private-photos-exposed-thanks-to-facebookflaw/[23/05/2012].

HIPAA 1996
Congress of the USA: *The Health insurance portability and accountability act*, In: Congress of the USA, 1996.

Ho/Kwok 2003
Ho, Shuk Ying/Kwok, Sai Ho: *The attraction of personalized service for users in mobile commerce: an empirical study, SIGecom Exch*. 3, 4: 10–18, 2003.

Ho/Tam 2005
Ho, S. Y./Tam, K. Y: *An Empirical Examination of the Effects of Web Personalization at Different Stages of Decision Making*, International Journal of Human-Computer Interaction, Vol. 19, Issue 1: 95–112, 2005.

Hoffman 2002
Hoffman, P: *RFC 3207: SMTP service extension for secure SMTP over Transport Layer Security*, The Internet Engineering Task Force, 2002.

Hu/Ahn 2011
Hu, Hongxin/Ahn, Gail-Joon: *Multiparty authorization framework for data sharing in online social networks,* Proceedings of the 25th annual IFIP WG 11.3 conference on Data and applications security and privacy (DBSec'11): , 29–43, Yingjiu Li (Ed.). Springer-Verlag, Berlin/Heidelberg, 2011.

Hu/Zong/Lee/Yeh 2003
Hu, Wen-Chen/Zong, Xuli /Lee, Chung-wei/ Yeh, Jyh-haw: *World Wide Web usage mining systems and technologies,* Journal on Systemics, Cybernetics, and Informatics, 1(4): 53–59, 2003.

Hull/Lipford/Latulipe 2011
Hull, Gordon/ Lipford, Heather Richter / Latulipe, Celine: *Contextual gaps: privacy issues on Facebook,* Ethics and Inf. Technol. Vol. 13, 4: 289–302, 2011.

IAB Europe 2010
Interactive Advertising Bureaux (IAB) Europe, *Europe's online ad market continues to grow despite the recession,* 2010. URL: http://www.iabeurope.eu/news/europe%27s-onlinead-market-continues-to-grow-despite-the-recession.aspx/ [26/05/2012].

IAB Europe 2011
Interactive Advertising Bureaux (IAB) Europe, *ONLINE DISPLAY ADVERTISING BOUNCES BACK*, 2011. URL: http://www.iabeurope.eu/news/online-display-advertising-bounces-back.aspx [26/05/2012].

IAB PWC 2011
PricewaterhouseCoopers, *IAB Internet Advertising Revenue Report,* 2011. URL:http://www.iab.net/insights_research/industry_data_and_landscape/adrevenuereport/ [26/05/2012].

ITU 2011
International Telecommunication Union, *Measuring the Information Society*, Geneva 2011.

InternetWorldStats 2011
Internet World Stats, *World Internet Usage and Population statistics,* 31/12/ 2011. URL: http://www.internetworldstats.com/stats.htm [26/07/2012].

Invoke 2010
Invoke, *Invoke Live! Social Commerce*, Key Findings Report, 15/10/ 2010. URL: http://www.invoke.com/sites/default/files/m-files/InvokeLive-2010-SocialCommerceReport.pdf/ [26/07/2012].

Irani/Webb/Li/Pu 2009
Irani, Danesh/ Webb,Steve/Li, Kang/ Pu, Calton: *Large Online Social Footprints–An Emerging Threat,* International Conference on Computational Science and Engineering 3: 271–276, 2009.

Irani/Webb/Pu/Li 2011
Irani, Danesh/Webb, Steve/Pu, Calton/Li, Kang: *Modeling Unintended Personal-Information Leakage from Multiple Online Social Networks*, Internet Computing, IEEE, Vol. 15, No. 3: 13–19, 2011.

Jagatic/Johnson/Jakobsson/Menczer 2007
Tom N. Jagatic, Nathaniel A. Johnson, Markus Jakobsson, and Filippo Menczer. 2007. Social phishing. Commun. ACM 50, 10 (October 2007), 94–100.

Jang/Jhala/Lerner/Shacham 2010
Jang, Dongseok/Jhala, Ranjit/Lerner, Sorin/Shacham, Hovav: *An empirical study of privacy-violating information flows in JavaScript web applications*, Proceedings of ACM conference on Computer and communications security (CCS ,10):270-283, 2010.

Jendricke/Markotten 2000
Jendricke, Uwe/Markotten, Daniela Gerd: *Usability meets security – the Identity-Manager as your personal security assistant for the Internet*, Proceedings of the 16th Annual Computer Security Applications Conference, IEEE Computer Society, 2000.

Johnson III 2007
Johnson III, Clay: *Safeguarding against and responding to the breach of personally identifiable information*, Office of Management and Budget Memorandum, 2007.

Jones/Kumar/Pang/Tomkins 2007
Jones, Rosie/Kumar, Ravi/Pang, Bo/Tomkins, Andrew: *„I know what you did last summer": query logs and user privacy, Proceedings of the sixteenth ACM conference on Conference on information and knowledge management* (CIKM ,07): 909–914, ACM, 2007.

John 2010
John, Jean: *Facebook CSRF and XSS vulnerabilities Destructive worms on a social network*, 05/10/2010. URL:http://www.john-jean.com/blog/advisories/facebook-csrf-and-xssvulnerabilities-destructive-worms-on-a-social-network-350/[26/07/2012].

Josang/Ismail/Boyd 2007
Josang, Audun/Ismail, Roslan/Boyd, Colin: A survey of trust and reputation systems for online service provision. In: Decision Support Systems, Vol. 43 Issue 2: 618-644, Elsevier Science Publishers, 2007.

Kamkar 2010
Kamkar, Samy: *Evercookie – never forget*, URL: http://samy.pl/evercookie/ [23/02.2012].

Kaushik 2007
Kaushik, Avinash: *Web Analytics: An Hour a Day*. SYBEX Inc., 2007.

Kaushik 2010
Kaushik, Avinash: *Web Analytics 2.0: The Art of Online Accountability and Science of Customer Centricity*, Wiley Publishing, Inc., 2010.

Kent/Seo 2005
Kent, S./Seo K.: RFC 4301: *Security Architecture for the Internet Protocol*. Internet Engineering Task Force, 2005.

Ko/Cheek/Shehab/Sandhu 2010
Ko, Moo Nam/Cheek, Gorrell P./Shehab, Mohamed/Sandhu, Ravi: *Social-Networks Connect Services,* Computer, Vol. 43, No.8: 37–43, 2010.

Kobsa 2001
Kobsa/Alfred: *Tailoring Privacy to Users' Need, Proceedings of the 8th International Conference on User Modeling 2001* (UM ,01): 303–313, Mathias Bauer, Piotr J. Gmytrasiewicz, and Julita Vassileva (Eds.). Springer-Verlag, London, 2001.

Kobsa 2003
Kobsa, Alfred: *A Component Architecture for Dynamically Managing Privacy Constraints in Personalized Web-Based Systems*, Privacy Enhancing Technologies:177–188, 2003.

Kobsa 2007
Kobsa, Alfred: Privacy-enhanced web personalization, In The adaptive web, Peter Brusilovsky, Alfred Kobsa, and Wolfgang Nejdl (Eds.), Lecture Notes In Computer Science, Vol. 4321: 628–670, Springer-Verlag, Berlin/Heidelberg, 2007.

Kolovski/Hendler 2007
Kolovski, Vladmimir/Hendler, James: *XACML Policy Analysis Using Description Logics*, Proceedings of the 15th International World Wide Web Conference: 494–497, 2007.

Krishnamurthy/Wills 2008
Krishnamurthy, Balachander/Wills, Craig: *Characterizing privacy in online social networks,* WOSN '08: Proceedings of the first workshop on Online social networks, 2008.

Krishnamurthy/Wills 2009
Krishnamurthy, Balachander/Wills, Craig : *On the Leakage of Personally Identifiable Information Via Online Social Networks,* Proceedings of ACM SIGCOMM Workshop on Online Social Networks, 2009.

Krishnamurthy/Wills 2010
Krishnamurthy, Balachander/Wills, Craig.E.: *Privacy leakage in mobile online social networks*, Proceedings of the 3rd conference on Online social networks, 4–4, 2010.

Kristol 2001
Kristol, David M.: *.HTTP Cookies: Standards, privacy, and politics*, ACM Trans. Internet Techn. 1(2): 151–198, 2001.

Kuhlmann/Gehring 2003
Kuhlmann, Dirk/Gehring, Robert A.: *Trusted Platforms, DRM, and Beyond,* In E. Becker, W. Buhse, D. Günnewig, &N. Rump (Eds.), Digital Rights Management Technological Economic Legal and Political Aspects: 178–205, Springer Berlin/Heidelberg, 2003.

Kundra 2011
Kundra, Vivek (US Chief Information Officer): *Federal Cloud Computing Strategy*, 8/2/2011. URL: http://www.cio.gov/documents/Federal-Cloud-Computing-Strategy.pdf [26/07/2012].

Korolova 2010
Korolova, A.: *Privacy Violations Using Microtargeted Ads* : A Case Study, Impressions: 27–49, 2010.

Köpsell 2010
Köpsell, Stefan: *Entwicklung und Betrieb eines Anonymisierungsdienstes für das WWW*, Dissertation, Technische Universität Dresden, 2010.

Landesman 2012
Landesman, Mary: *Browser History Sniffing and Other Tracking Techniques*. URL: http://antivirus.about.com/od/securitytips/a/historysniffing.htm/ [23/02/2012].

Lardinois 2010
F. Lardinois: *PleaseRobMe and the Dangers of Location-Based Social Networks,* ReadWriteWeb, 02/2010. URL: http://www.readwriteweb.com/archives/pleaserobme_and_the_dangers_of_location-aware_social_networks.php/ [26/07/2012].

Langheinrich/Karjoth 2011
Langheinrich, Marc/Karjoth, Günter: *Social Networking and the Risk to Companies and Institutions*, In Information Security Technical Report, Special Issue: Identity Reconstruction and Theft, Issue 15 (2010):51–56, Elsevier, 2011.

Larsen 2008
Larsen, Niels Elgaard: *Privacy in The Polippix Project*, IT-Political Association of Denmark (IT-POL), 2008.

Lee 2006
Lee, E.A: *Cyber-Physical Systems – Are Computing Foundations Adequate?* 1–6, 2006.

Lee 2008
Lee, E.: *Cyber physical systems: Design challenges*, IEEE International Symposium Object Oriented Real-Time Distributed Computing (ISORC): 363–369, 2008.

Leech/Ganis/Lee/Kuris/Koblas/Jones 1996
Leech, M/Ganis, M/Lee, Y/Kuris, R/Koblas, D/Jones, L: *RFC 1928: SOCKS Protocol Version 5*. The Internet Engineering Task Force, 1996.

Leenes/Schallaböck/Hansen 2008
Leenes, Ronald/Schallaböck, Jan/Hansen, Marit: *PRIME White Paper*. PRIME (Privacy and Identity Management for Europe), 2008.

Li/Li/Venkatasubramanian 2007
Li, Ninghui/Li, Tiancheng/Venkatasubramanian, Suresh: *t-closeness: Privacy beyond k-anonymity and ldiversity*, Data Engineering, Vol. 3: 106–115, 2007.

Li/Chen 2010
Li, Nan/Chen, Guanling: *Sharing location in online social networks*, Network, IEEE, Vol. 24, No. 5: 20–25, 2010.

Löhr/Ramasamy/Sadeghi/Schulz/Schunter/Stüble 2007
Löhr, Hans/Ramasamy, HariGovind V./Sadeghi, Ahmad-Reza/Schulz, Stefan/Schunter, Matthias/Stüble, Christian: *Enhancing Grid Security Using Trusted Virtualization*, Lecture Notes in Computer Science, Vol. 4610: 372–384, 2007.

Lotan/Graeff/Ananny/Gaffney/Pearce/boyd 2011
Lotan, G./Graeff, E./Ananny, M./Gaffney, D./Pearce, I./boyd, d.: *The Revolutions Were Tweeted: Information Flows During the 2011 Tunisian and Egyptian Revolutions.* International Journal of Communications, Vol. 5: 1375–1405, 2011.

Ma/Zhou/Lyu /King 2011
Ma, Hao/Zhou, Tom Chao/Lyu, Michael R./King, Irwin: *Improving Recommender Systems by Incorporating Social Contextual Information, ACM Trans. Inf. Syst.* 29, Vol. 2, Article 9, 2011.

Machanavajjhala/Gehrke/Kifer 2007
Machanavajjhala, Ashwin/Gehrke, Johannes/Kifer, Daniel: *L-diversity: Privacy beyond k-anonymity,* ACM Transactions on Knowledge Discovery from Data (TKDD), Vol. 1, Issue 1, 2007.

Machanavajjhala/Kifer/Gehrke/Venkitasubramaniam 2007
Machanavajjhala, Ashwin/Kifer, Daniel/Gehrke, Johannes/Venkitasubramaniam, Muthuramakrishnan: *L-diversity: Privacy beyond k-anonymity,* ACM Transactions on Knowledge Discovery from Data, Vol. 1, Issue 1, 2007.

Machanavajjhala/Korolova/Sarma 2011
Machanavajjhala, Ashwin/Korolova, Aleksandra/Das Sarma, Atish: Personalized Social Recommendations – Accurate or Private?, Journal Proceedings of the VLDB Endowment, Vol. 4, Issue 7, April 2011.

Madria/Bhowmick/Ng/Lim 1999
Madria,Sanjay Kumar/Bhowmick, Sourav S./Ng, Wee Keong/Lim, Ee-Peng: *Research Issues in Web Data Mining*, in Proceedings of Data Warehousing and Knowledge Discovery, DaWaK 1999.

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

Manyika/Chui/Brown/Bughin/Dobbs/Roxburgh/Byers 2011
Manyika, James/Chui, Michael/Brown, Brad/Bughin, Jacques/Dobbs, Richard/Roxburgh, Charles/Byers, Angela Hung: Big data: *The next frontier for innovation, competition, and productivity*, McKinsey Global Institute, 2011. URL: http://www.mckinsey.com/Insights/MGI/Research/Technology_and_Innovation/Big_data_The_next_frontier_for_innovation

Masiello/Whitten 2010
Masiello, Betsy/Whitten, Alma: Engineering Privacy in an Age of Information Abundance, Intelligent Information Privacy Management: 119–24, 2010.

Marlinspike 2009
Marlinspike, M.: *New Techniques for Defeating SSL/TLS,* Black Hat DC, 2009. URL: http://www.blackhat.com/presentations/bh-dc-09/Marlinspike/BlackHat-DC-09-Marlinspike-Defeating-SSL.pdf

Madden 2012
Madden, Mary: *"Privacy Management on Social Media Sites,"* The Pew Research Center's Internet and American Life Project, 2012.

McCallister/Grance/Scarfone 2010
McCallister, E./Grance, T./Scarfone, K.: Guide to Protecting the Confidentiality of Personally Identifiable Information (PII), NIST Special Publication. U.S. Dept. of Commerce, National Institute of Standards and Technology, 2010.

McCoy/Bauer/Grunwald/Kohno/Sicker 2008
McCoy, Damon/Bauer, Kevin/Grunwald, Dirk/Kohno, Tadayoshi/Sicker, Douglas: Shining Light in Dark Places: *Understanding the Tor Network,* Proceedings of the 8th international symposium on Privacy Enhancing Technologies: 63–76, Springer-Verlag, Berlin, Heidelberg, 2008.

McDonald/Cranor 2008
McDonald, A./Cranor, L.: *The Cost of Reading Privacy Policies,* In Technology Policy Research Conf., 2008.

McKinley 2008
McKinley, Katherine: Cleaning Up After Cookies Version I.0, San Francisco 2008.

McSherry/Mironov 2009
McSherry, Frank/Mironov, Ilya: *Differentially private recommender systems: building privacy into the ne, Proceedings of the 15th ACM SIGKDD international conference on Knowledge discovery and data mining* (KDD ,09): 627–636, ACM, 2009.

Menezes/Oorschot/Vanstone 1996
Menezes, Alfred J/Van Oorschot, Paul C/Vanstone, Scott A: *Handbook of Applied Cryptography,* CRC Press, 1996.

Meyer 2011
Meyer, David: *The Schleswig-Holstein Question,* BBC News. 10/09/2011. URL: http://www.bbc.co.uk/news/technology-14859813

Mills 2011
Mills, Elinor: Hackers release credit card, other data from Stratfor breach, CNET News, 30/12/2011. URL: http://news.cnet.com/8301-27080_3-57350361-245/hackersrelease-credit-card-other-data-from-stratfor-breach/ [26/07/2012].

Mobasher/Dai/Luo/Sun/Zhu 2000
Mobasher, Bamshad/Dai, Honghua/Luo, Tao/Sun, Yuqing/Zhu, Jiang: *Integrating Web Usage and Content Mining for More Effective Personalization*, Proceedings of the First International Conference on Electronic Commerce and Web Technologies (EC-WEB ,00),. Springer-Verlag, London, 2000.

Mobasher 2007
Mobasher, Bamshad: *Data Mining for Web Personalization,* In The Adaptive Web: Methods and Strategies of Web Personalization, Brusilovsky, P., Kobsa, A., Nejdl, W. (eds.). Brusilovsky, P., Kobsa, A., Nejdl, W. (eds.). Lecture Notes in Computer Science, Vol. 4321: 90–135, Springer, Berlin/Heidelberg, 2007.

Mochalski/Schulze 2009
Mochalski, Klaus/Schulze, Hendrik: *Deep Packet Inspection – Technology, Applications & Net Neutrality,* Forum American Bar Association, Vol. 24, Issue 1, 2010.

Mui/Mohtashemi/Halberstadt 2002
Mui, Lik/Mohtashemi, Mojdeh/Halberstadt, Ari: *A Computational Model of Trust and Reputation for E-businesses, Proceedings of the 35th Annual Hawaii International Conference on System Sciences*, Volume 7: 2431–2439, IEEE Computer Society, 2002.

Murphy/Salomone 2010
Murphy, Glen D./Salomone, Sonia: *Using Enterprise 2.0 tools to facilitate knowledge transfer in complex engineering environments*, 2010.

Narayanan/Shmatikov 2008
Narayanan, Arvind/Shmatikov, Vitaly: *Robust Deanonymization of Large Sparse Datasets, Proceedings of the IEEE Symposium on Security and Privacy* (SP ,08): 111–125, IEEE Computer Society, 2008.

Narayanan/Shmatikov 2009
Narayanan, Arvind/Shmatikov, Vitaly: *De-anonymizing Social Networks*, IEEE S&P 2009.

Newman 1999
Newman, C: RFC 2595: *Using TLS with IMAP, POP3 and ACAP,* 1999.

Ni/Bertino/Lobo/Calo 2009
Ni, Qun/Bertino, Elisa/Lobo, Jorge/Calo, Seraphin B: *Privacy-Aware Role Based Access Control,* IEEE Security & Privacy, Vol. 7, Issue 4: 35–43, 2009.

Nielsen 2009
The Nielsen Company, *Social Networking and Blog Sites Capture More Internet Time and Advertising,* 2009. URL:http://blog.nielsen.com/nielsenwire/online_mobile/social-networking-and-blog-sites-capture-more-internet-time-and-advertisinga/ [23/05/2012].

Nielsen 2010
Nielsenwire, *Social Networks/Blogs Now Account for One in Every Four and a Half Minutes Online*, 2010. URL:http://blog.nielsen.com/nielsenwire/global/social-mediaaccounts-for-22-percent-of-time-online/[23/05/2012].

Nielsen 2011
Nielsen: *Social Media Report: Q3*, 2011. URL: http://blog.nielsen.com/nielsenwire/social/[23/05/2012].

Nissenbaum 2010
Nissenbaum/ Helen: *Privacy in Context: Technology, Policy, and the Integrity of Social Life*, Palo Alto, CA: Stanford University Press, 2010.

NETL 2009
National Energy Technology Laboratory (NETL), *The Modern Grid Strategy Vision,* 2009. URL: http://www.netl.doe.gov/moderngrid/vision.html/[23/05/2012].

NISTIR 7628
The Smart Grid Interoperability Panel-Cyber Security Working Group, Smart grid cyber security strategy and requirements (draft nistir 7628), The National Institute of Standards and Technology (NIST), Tech. Rep., 2010.

Nofer/Hinz/Muntermann/Roßnagel 2011
Nofer, Michael/Hinz, Oliver/Muntermann, Jan/Roßnagel, Heiko: *Assessing the Economic Impact of Privacy Violations and Security Breaches – The Case of the Financial Industry,* TU Darmstadt , Germany, 2011.

nVision 2008
nVision: *E-commerce across Europe-Progress and prospects,* London, UK, 2008.

Owad 2006
Owad, Tom: *Data Mining 101: Finding Subversives with Amazon Wishlists,* 04/01/2006. URL: http://www.applefritter.com/bannedbooks

Page/Brin/Motwani/Winograd 1998
Page, Lawrence/Brin, Sergey/Motwani, Rajeev/Winograd, Terry: *The PageRank Citation Ranking: Bringing Order to the Web*, Technical Report, Stanford InfoLab, 1998.

Pamnani/Chawan 2010
Pamnani, Rajni/Chawan, Pramila: *Web Usage Mining: A Research Area in Web Mining,* International Conference on Recent Trends in Computer Engineering, ISCET, RIMT, 2010.

Park/Sandhu 2002
Park, Jaehong/Sandhu, Ravi: *Towards usage control models: beyond traditional access control,* Proceedings of the seventh ACM symposium on Access control models and technologies: 57–64, ACM, New York, NY, USA, 2002.

Peterson 2010
Peterson, P.A.H.: *Cryptkeeper: Improving security with encrypted RAM,* IEEE International Conference on Technologies for Homeland Security: 120–126, 2010.

PCAST 2010
Executive Office of the President President's Council of Advisors on Science and Technology (PCAST), REPORT TO THE PRESIDENT AND CONGRESS DESIGNING A DIGITAL FUTURE: FEDERALLY FUNDED RESEARCH AND DEVELOPMENT IN NETWORKING AND INFORMATION TECHNOLOGY, DECEMBER 2010, http://www.whitehouse.gov/sites/default/files/microsites/ostp/pcast-nitrd-report-2010.pdf

Pfitzmann/Hansen 2010
Pfitzmann, Andreas/Hansen, Marit: *A terminology for talking about privacy by data minimization: Anonymity, Unlinkability, Undetectability, Unobservability, Pseudonymity, and Identity Management,* Internet-Draft, 2010.

Pike Research 2011.
Pike Research, Smart Grid Data Analytics, 2011. URL: http://www.pikeresearch.com/research/smart-grid-data-analytics

Powers/Ashley/Schunter 2002
Powers, Calvin S/Ashley Paul/Schunter Matthias: *Privacy Promises, Access Control, and Privacy Management. Enforcing Privacy Throughout an Enterprise by Extending Access Control,* Proceedings Third International Symposium on Electronic Commerce: 13–21, IEEE, 2002.

Primelife 2011
Raggett, Dave (ed.): *Privacy Enhancing Browser Extensions Deliverable:* D 1.2.3., 28/2/2011. URL: http://www.w3.org/2011/D1.2.3/

PWC 2011
Jacobson, David: *Digital mobility drives you-You drive digital mobility, PricewaterhouseCoopers,* 2011. URL: http://www.pwc.com/ca/en/technology-consulting/technology-advisory/digital-mobility-white-paper.jhtml

Quinn 2009
E. L. Quinn: *Privacy and the new energy infrastructure*, 2/2009. URL: http://ssrn.com/abstract=1370731.

Ramakrishnan/Keller/Mirza/Grama/Karypis 2001
Ramakrishnan, Naren/Keller, Benjamin J./Mirza, Batul J./Grama, Ananth Y./Karypis, George: *Privacy Risks in Recommender Systems,* Journal IEEE Internet Computing, Volume 5, Issue 6, IEEE Educational Activities Department Piscataway, 2001.

Raice 2011
Raice, Shayndi: *LinkedIn Retreats in Privacy Flap*, The Wall Street Journal, 8/2011. URL: http://online.wsj.com/article/SB10001424053111904823804576502860557223074.html

Rao/Rohatgi 2000
Rao, Josyula R./Rohatgi, Pankaj: *Can Pseudonymity Really Guarantee Privacy?*, Proceedings of the 9th conference on USENIX Security Symposium, Vol. 9: 85–96, USENIX Association, 2000.

Reed/Syverson/Goldschlag 1998
Reed, Michael/Syverson, Paul/Goldschlag, David: *Anonymous connections and onion routing,* IEEE Journal on Selected Areas in Communications, Vol. 16, Issue 4: 482–494, 1998.

Rescorla 2000
Rescorla, Eric: RFC 2818: *HTTP Over TLS.* The Internet Engineering Task Force, 2000.

Resnick/Varian 1997
Resnick, P./Varian, H. R.: Recommender Systems, Magazine Communications of the ACM, Vol. 40, Issue 3, ACM, 1997.

Resnick/Zeckhauser/Friedman/Kuwabara 2000
Resnick, Paul/Kuwabara, Ko/Zeckhauser, Richard/Friedman, Eric: *Reputation systems,* Communications of the ACM, Vol. 43 Issue 12: 45–48, 2000.

Rifkind 2010
Rifkind, Malcolm: *WikiLeaks: Do they have a right to privacy?,* The Telegraph, 30/11/2010. URL: http://www.telegraph.co.uk/news/worldnews/wikileaks/8169712/WikiLeaks-Do-they-have-a-right-to-privacy.html

Rivest/Shamir/Adleman 1978
Rivest, Ronald L/Shamir, Adi/Adleman, Leonard: *A method for obtaining digital signatures and public-key cryptosystems,* Communications of the ACM, Vol. 21 Issue 2: 120-126, 1978.

Rosen 2010
Rosen, Jeffrey: *The Web Means the End of Forgetting,* The New York Times, 25/ 07/2010. URL: http://www.nytimes.com/2010/07/25/magazine/25privacy-t2.html?pagewanted=all/ [23.02.2012].

Rosteck 2008
Rosteck, Thomas: *Die Trusted Computing Group,* Trusted Computing: 15–20, Vieweg+Teubner, 2008.

Sabater/Sierra 2005
Sabater, Jordi/Sierra, Carles: *Review on Computational Trust and Reputation Models, Artificial Intelligence Review,* Vol. 24 Issue 1: 33–60, 2005.

Sackmann/Strüker/Accorsi 2006
Sackmann, Stefan/Strüker, Jens/Accorsi, Rafael: *Personalization in privacy-aware highly dynamic systems.* In: Communications of the ACM – Privacy and security in highly dynamic systems, Vol. 49 Issue 9: 32–38, ACM, 2006.

Sandhu/Coyne/Feinstein/Youman 1996
Sandhu, Ravi S/Coyne, Edward J/Feinstein, Hal L/Youman, Charles E: *Role-Based Access Control Models.* In: Journal Computer, Vol. 29 Issue 2: 38–47, 1996.

Sandhu/Samarati 1994
Sandhu, Ravi S/Samarati, Pierangela: *Access control: principle and practice.* In: Communications Magazine, IEEE, Vol. 32 No. 9: 40–48, 1994.

Sarbanes-Oxley 2002
SOX (2002) Sarbanes-Oxley act, In: Congress of the USA, 2002.

Schäfers 2008
Schäfers, B.: *E-Commerce in der Otto-Group am Beispiel des Social Shopping-Portals*, Handbuch Kundenmanagement: 677–685, 2008.

Schenker 2003
Schenker, Adam: *Graph-Theoretic Techniques for Web Content Mining,* dissertation for the degree of Doctor of Philosophy, Department of Computer Science and Engineering, College of Engineering, University of South Florida, 2003.

Schmücker 2011
Schmücker, Niklas: *Web Tracking,* SNET2 Seminar Paper, TU Berlin, Germany, 2011.

Schneier 1993
Schneier, Bruce: *Description of a New Variable-Length Key,* 64-bit Block Cipher (Blowfish), Fast Software Encryption, Cambridge Security Workshop: 191–204, Springer, London, 1993.

Schneier 2010
Schneier, Bruce: *A Taxonomy of Social Networking Data,* In Journal IEEE Security and Privacy, Vol. 8, Issue 4, 2010.

Schoemaker 2011
Schoemaker, René: *LinkedIn's Privacy Slip-up Draws Legal Scrutiny,* (PCWorld), 2011. URL: http://www.pcworld.com/article/237849/linkedins_privacy_slipup_draws_legal_scrutiny.html

Seneviratne/Kagal 2011
Seneviratne, Oshani/Kagal, Lalana: *Usage Restriction Management for Accountable Data Transfer on the Web*, 2011.

Sheng/Nah/Siau 2008
Sheng, Hong/Nah, Fiona Fui-Hoon/Siau, Keng: *An Experimental Study on U-commerce Adoption: The Impact of Personalization and Privacy Concerns,* Journal of Associations for Information Systems (JAIS), Vol. 9, Issue 6, Article 15, 2008.

Shmatikov/Talcott 2005
Shmatikov, Vitaly/Talcott, Carolyn: *Reputation-based trust management*, Journal of Computer Security, Vol. 13 No. : 167–190, 2005.

Smith 1982
Smith, Alan Jay: *Cache Memories*, ACM Computing Surveys (CSUR), Vol. 14, No. 3, 1982.

Smyth/Coyle/Briggs 2011
Smyth, Barry/Coyle, Maurice/Briggs, Peter: *Communities, Collaboration, and Recommender Systems in Personalized Web Search*, Recommender Systems Handbook, Part 4: 579–614, Springer Verlag, 2011.

Singel 2009
Singel, Ryan: *You Deleted Your Cookies?* Think Again. URL: http://www.wired.com/business/2009/08/you-deleted-your-cookies-think-again/ [23.02.2012] .

Soghoian/Stamm 2010
Soghoian, C./Stamm, S.: Certified Lies: Detecting and Defeating Government Interception Attacks Against SSL, papersssrncom: 1–19, 2010. URL: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1591033

Solove 1972
Solove, Daniel J.: *Understanding Privacy,* Harvard University Press, 1972 (New Edition 2008).

Soltani/Canty/Mayo/Thomas/Hoofnagle 2009
Soltani, Ashkan/Canty, Shannon/Mayo, Quentin/Thomas, Lauren/Hoofnagle, Chris Jay: *Flash Cookies and Privacy,* SSRN, 2009.

Sophos 2010
Sophos, Facebook Worm – Likejacking, 31/05/2010. URL: http://nakedsecurity.sophos.com/2010/05/31/facebook-likejacking-worm/ [26/072012].

Stackoverflow 2010
How do I use cookies to store users' recent site history (PHP)? URL: http://stackoverflow.com/questions/2813659/how-do-i-usecookies-to-store-users-recent-site-historyphp/ [23.02.2012].

Steinbrecher/Koepsell 2003
Steinbrecher, Sandra/Koepsell, Stefan: *Modelling Unlinkability,* Privacy Enhancing Technologies, Vol. 2760: 32–47, Springer Berlin/Heidelberg, 2003.

Steindel 2011
Steindel, Tracy A.: *A Path Toward User Control of Online Profiling,* 17 Mich. Telecomm. Tech. L. Rev. 459, 2010.

Sweeney 1997
Sweeney, Latanya: *Weaving Technology and Policy Together to Maintain Confidentiality,* 25 J.L. MED. & ETHICS 98, 100, 1997. ("The term anonymous implies that the data cannot be manipulated or linked to identify an individual." (emphasis in original)).

Sweeney (1) 2002
Sweeney, Latanya: *Achieving k-Anonymity Privacy Protection Using Generalization and Suppression,* 10 INT'L J. on Uncertainty, Fuzziness and Knowledge-based Systems: 571–572, 2002.

Sweeney (2) 2002
Sweeney, Latanya: k-anonymity: *A model for protecting privacy,* International Journal on Uncertainty Fuzziness and Knowledge-based Systems, Vol. 10, Issue 5: 557–570, 2002.

Tam/Ho 2003
Tam, Kar Yan/Ho, Shuk Ying: *Web personalization: is it effective?*, IT Professional, Vol. 5, No. 5: 53–57, 2003.

Tam/Ho 2005
Tam, Kar Yan/Ho, Shuk Ying: *Web Personalization as a Persuasion Strategy:* An Elaboration Likelihood Model Perspective, Information Systems Research, Vol. 16, Issue 3, INFORMS Institute for Operations Research and the Management Sciences (INFORMS), Linthicum, 2005.

Tan/Steinbach/Kumar 2006
Tan, Pang-Ning/Steinbach, Michael/Kumar, Vipin: *Introduction to Data Mining,* Addison Wesley, 2005.

Tarasewich/Nickerson/Warkentin 2002
Tarasewich, Peter/Nickerson, Robert C./Warkentin, Merrill: *Issues in Mobile E-Commerce,* Communications of the Association for Information Systems: Vol. 8, Article 3, 2002.

Tene/Polonetsky 2012
Tene, Omer/Polonetsky, Jules: *To Track or 'Do Not Track':* Advancing Transparency and Individual Control in Online Behavioral Advertising, 2011. URL: http://ssrn.com/abstract=1920505

Teltzrow/Kobsa 2004
Teltzrow, Maximilian/Kobsa, Alfred: *Impacts of user privacy preferences on personalized systems:* a comparative study, Designing personalized user experiences in eCommerce, Kluwer Academic Publishers, 2004.

Thearling 2000
Thearling, Kurt: *Data warehousing,* 2000. URL: http://www.thearling.com/text/hrdotcom/dw.htm/ [23/05/2012].

Tirtea/Castelluccia/Ikonomou 2011
Tirtea, Rodica/Castelluccia, Claude/Ikonomou, Demosthenes: *Bittersweet cookies, Some security and privacy considerations,* European Network, and information Security Agency (ENISA), 2011.

Thompson/Hall 2010
Thompson, K. D. Catherine/Hall, Jim: *Privacy by Design: Achieving the Gold Standard in Data Protection for the Smart Grid,* June 2010.

Tomlinson/Yau/MacDonald 2010
Tomlinson, Allan/Yau, Po-Wah/MacDonald, John A.: *Privacy threats in a mobile enterprise social network,* Information Security, Technical Report 15: 57–66, 2010.

Toubiana/Narayanan/Boneh/Nissenbaum/Barocas 2010
Toubiana, Vincent/Narayanan, Arvind/Boneh, Dan/Nissenbaum, Helen: *Adnostic: Privacy preserving targeted advertising,* Proceedings of the Network and Distributed Systems Symposium, 2010.

Toubiana/Nissenbaum 2011
Toubiana, Vincent/Nissenbaum, Helen: *An Analysis of Google Log Retention Policies,* Journal of Privacy and Confidentiality, Vol. 3, Issue 1, Article 2, 2011.

Trowbridge 2003
Trowbridge, Chris: *An Overview of Remote Operating System Fingerprinting,* Sans Institute, 2003.

Tuffield 2007
M. Tuffield: *NHS.uk allowing Google, Facebook, and others to track you*. URL: http://mmt.me.uk/blog/2010/11/21/nhs-and-tracking/ [26/072012].

Turow/King/Hoofnagle/Bleakley/Hennessy 2009
Turow, Joseph/King, Jennifer/Hoofnagle, Chris Jay/Bleakley, Amy/Hennessy, Michael: *Americans Reject Tailored Advertising and Three Activities that Enable It,* Social Science Research Network, Vol. 104, Issue 30: 1–27, 2009.

ULD 2011
Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein (ULD): *Wer ist datenschutzrechtlich verantwortlich für Facebook-Fanpages und Social-Plugins?* URL: https://www.datenschutzzentrum.de/facebook/facebook-verantwortlichkeit.html [02/01/2012]

UscourtsNo.07-1660 2008.
Stacey Snyder Plaintiff v. Millersville University et al., The US District Court for the Eastern District of Pennsylvania (NO.07-1660), 3/12/2008. URL: http://www.paed.uscourts.gov/documents/opinions/08d1410p.pdf

Vaas 2012
Vaas, Lisa: *"Deleted" Facebook photos survive online three years later, Sophos security blog*, 8/02/2012. URL: http://nakedsecurity.sophos.com/2012/02/08/deleted-facebook-photos-survive/

Vascellaro 2009
Vascellaro, Jessica E.: *Facebook's About-Face on Data,* The Wall Street Journal, 19/02/2009. URL: http://online.wsj.com/article/SB123494484088908625.html

Vega 2011
Vega, Tanzina: *AT&T Begins Service to Text Users in Certain Locations,* The New York Times, 27/02/2011. URL: http://mediadecoder.blogs.nytimes.com/2011/02/27/att-begins-service-to-text-users-in-certain-locations/ [26/072012].

Venzke 2011
Venzke, Sven: *Social Media Marketing: Eine datenschutzrechtliche Orientierungshilfe,* 2011. URL: http://www.datenschutz-nord.de/presse/download/Rahmenbedingungen_Social_Media_Marketing_DuD_062011.pdf

Vratonjic/Manshaei/Raya/Hubaux 2010
Vratonjic, N./Manshaei, M./Raya, M.,/Hubaux, J. P.: *ISPs and Ad Networks Against Botnet Ad Fraud,* Proceedings of the First international conference on Decision and game theory for security (GameSec'10): 149–167, Springer-Verlag, Berli/Heidelberg, 2010

W3C 2010
W3C, *Same Orighin Policy,* 2010. URL: http://www.w3.org/Security/wiki/Same_Origin_Policy [23.02.2012].

Walters 2009
Walters, Chris: *Facebook's New Terms Of Service: "We Can Do Anything We Want With Your Content. Forever.",* 2/2009. URL: http://consumerist.com/2009/02/facebooks-new-terms-of-service-we-can-do-anything-we-want-with-your-content-forever.html [26/072012].

Weinberg/Chen/Jayaraman/Jackson 2011
Weinberg, Zachary/Chen, Eric Y./Jayaraman, Pavithra Ramesh/ Jackson, Collin: *I Still Know What You Visited Last Summer: Leaking Browsing History via User Interaction and Side Channel Attacks,* IEEE Security and Privacy (SP) Symposium: 147–161, 2011.

Weitzner/Abelson/Berners-Lee/Hanson/Hendler/Kagal/McGuinness/Sussman/Waterman 2006
Weitzner, Daniel J./Abelson, Harold/Berners-Lee, Tim/ Hanson, Chris/Hendler, James/Kagal, Lalana/McGuinness, Deborah L/Sussman, Gerald Jay/Waterman, K Krasnow: *Transparent Accountable Data Mining: New Strategies for Privacy Protection,* Computer Science and Artificial Intelligence Laboratory, Technical Report MIT-CSAIL-TR-2006-007, 2006.

Whalen 2002
David Whalen: *The Unofficial Cookie FAQ, Version 2.6*. URL: http://www.cookiecentral.com/faq/ [23.02.2012].

Winkler 2006
William E., Winkler/ William E., Winkler/P., Nov: *Overview of record linkage and current research directions,* Technical report, Bureau of the Census, 2006.

Wondracek/Holz/Kirda/Kruegel 2010
Wondracek, G./Holz, T./Kirda, E./Kruegel, C.: *A practical attack to de-anonymize social network users,* IEEE Symposium on Security and Privacy: 223–238, 2010.

Wong/Fu/Wang/Yu/Pei 2011
Wong, Raymond Chi-Wing/Fu, Ada Wai-Chee/Wang, Ke/ Yu, Philip/Pei, Jian: *Can the Utility of Anonymized Data be used for Privacy Breaches?,* ACM Transactions on Knowledge Discovery from Data (TKDD), Vol. 5, Issue 3, 2011.

Yung 2003
Yung, Moti: *Trusted computing platforms: the good, the bad, and the ugly.* In: Computer Aided Verification, Lecture Notes in Computer Science, Vol. 2742: 250–254, Springer, 2003.

Zarsky 2003
Zarsky, Tal Z.: *Thinking Outside the Box: Considering Transparency, Anonymity, and Pseudonymity as Overall Solutions to the Problems of Information Privacy in the Internet Society.* In University of Miami Law Review, Vol. 58, Issue 4: 1301–1354, 2004.

Zeh 2011
Zeh, Reimar: *Wie viele Fans hat Angela Merkel? Wahlkampf in Social Network Sites, Die Massenmedien im Wahlkampf,* VS Verlag für Sozialwissenschaften, 2010.

Zeller 2006
Zeller, Tom Jr.: *AOL Executive Quits After Posting of Search Data*, New York Times, 2010.

Zheleva/Getoor 2009
Zheleva, E./Getoor, L.: *To join or not to join: The illusion of privacy in social networks with mixed public and private user profiles,* International World Wide Web Conference (WWW), 2009.

Zimmerman 1995
Philip Zimmermann: *PGP Source Code and Internals*, MIT Press, 1995.

Zimmermann 1980
Zimmermann, Hubert: *OSI Reference Model – The ISO Model of Architecture for Open Systems Interconnection,* IEEE Transactions on Communications, Vol. 28, Issue 4: 425–432, 1980.

Zwass 1996
Zwass, Vladimir: *Electronic commerce: structures and Issues,* In Journal International Journal of Electronic Commerce, Vol. 1:3–23, 1996.

5 INTERNET PRIVACY AUS RECHTSWISSENSCHAFTLICHER SICHT

ALEXANDER ROSSNAGEL, PHILIPP RICHTER, MAXI NEBEL

ZUSAMMENFASSUNG

Der Beitrag untersucht die rechtlichen Rahmenbedingungen für eine Kultur der Privatsphäre und des Vertrauens im Internet. Zunächst wird geklärt, welche Bedeutung den Begriffen *Kultur* und *Vertrauen* im Recht zukommt. Ausgehend von der Feststellung, dass unter *Privatsphäre* als solche im deutschen Recht kein einheitliches Schutzkonzept oder Rechtsgut verstanden wird, werden die verfassungsrechtlichen Schutzgüter auf nationaler und europäischer Ebene vorgestellt, die im Zusammenhang mit Anwendungsszenarien im Internet berührt werden. Diese Szenarien werden sodann auf ihre Chancen und Risiken bezüglich der verfassungsrechtlichen Schutzgüter hin untersucht. Anschließend wird ein Überblick über die aktuelle Rechtslage in Deutschland unter Berücksichtigung der Vorgaben auf europäischer Ebene gegeben. Zum Schluss erhält der Leser einen Überblick über die seit Jahren anhaltende Modernisierungsdiskussion für ein zeitgemäßes Datenschutzrecht und über aktuelle Reformvorhaben.

ABSTRACT

This article analyzes the legal framework for a culture of privacy and trust on the Internet. Firstly, the definitions of the terms *culture* and *trust* will be clarified in a legal context. Since *privacy* does not describe a consistent protection concept or legal position in German law, the authors then describe which constitutional specifications on national and European levels come into play within application scenarios on the internet. The opportunities and risks pertaining to these scenarios are then analyzed with regard to constitutional protection. Then follows an overview of the legal situation in Germany, including broader European standards. Finally, the reader will be given an overview of the on-going debate over today's regulation of data protection and of current legislative proposals.

5.1 EINFÜHRUNG

5.1.1 ZIELSETZUNG UND RELEVANZ IN BEZUG AUF DAS PROJEKT

Im rechtlichen Abschnitt des *Status Quo* soll aufgezeigt werden, wie und inwiefern eine *Kultur der Privatsphäre und des Vertrauens im Internet* bisher durch demokratisch legitimierte Prozesse in verbindlichen Freiheitsrechten und Gesetzen konkretisiert wurde und welche Modernisierungsvorschläge hierzu bestehen.

Zunächst wird das Verhältnis des Rechts zu den zentralen Begriffen des Projekts *Kultur, „Privacy/Privatsphäre"* und *Vertrauen* mit Bezug zum Internet herausgearbeitet. Hierzu werden vor allem die in Deutschland und Europa einschlägigen Grund- und Menschenrechte erläutert. Anschließend werden die von der Technik in den fünf Anwendungsszenarien: *„Personalized Web und E-Commerce"*, *„Social Networks"*, *„Cloud Computing"*, *„Big Data"* und *„Ubiquitous Computing"* als *„Privacy Breach"* identifizierten Handlungen und Phänomene auf diese Schutzgüter bezogen, um festzustellen, ob das Recht sie als Beschränkung der einschlägigen Freiheitsgüter bewertet. Auch die Chancen, die sich für Schutzgüter in den Anwendungsszenarien ergeben, werden aufgezeigt, um darzustellen, welche Rechtspositionen sich im Einzelnen gegenüberstehen. Anschließend wird die aktuelle einfachgesetzliche Rechtslage im Bereich des Datenschutzes im Internet erläutert, die die konkrete Verwirklichung der abstrakten Schutzgüter gewährleisten soll. Dies geschieht einerseits, um Nichtjuristen einen Überblick über die datenschutzrechtlichen Anforderungen für Dienste in den Anwendungsszenarien zu verschaffen, andererseits um die Identifizierung von Schutzlücken im Hinblick auf die aktuellen Risiken vorzubereiten.

Überdies wird der Stand der Diskussion einer Modernisierung des Datenschutzrechts aufgearbeitet. Hierzu werden die wichtigsten größeren Beiträge und aktuelle Gesetzgebungsvorhaben zusammengefasst. Dieser Abschnitt hat das Ziel, die anschließende Identifizierung von Schutzdefiziten des aktuellen Datenschutzrechts und die Anforderungsanalyse für ein modernes Datenschutzrecht, das eine Vertrauenskultur im Internet fördert, auf der Höhe der Diskussion zu beginnen.

5.1.2 KULTUR UND RECHT

Kultur im Sinne des Projekts meint nicht die Hochkultur im Sinne von bildender Kunst und Wissenschaft, sondern die Alltagskultur im Sinne von gesellschaftlichen Gebräuchen und Gewohnheiten. Der Begriff Kultur ist durch das Recht nicht in bestimmter Weise belegt. Zwar können viele, insbesondere die in Art. 5 des Grundgesetzes (GG) garantierten Grundrechte als Vorbedingungen für die Entstehung bestimmter Kulturformen angesehen werden. Der Begriff Kultur wird auch vereinzelt im deutschen Grundgesetz verwendet, namentlich in Art. 23 Abs. 6 Satz 1, Art. 29 Abs. 2 Satz 2, Art. 73 Abs. 1 Nr. 5a und 89 Abs. 3 GG, dies aber mit jeweils unterschiedlicher Bedeutung: einmal im Sinne der Hochkultur, einmal im Sinne der Alltagskultur.

Im Hinblick auf die Internetnutzung lässt sich sagen: Das deutsche Recht und das EU-Recht (hier in erster Linie das Datenschutzrecht) normieren eine bestimmte Kultur der Privatsphäre und des Vertrauens im Internet, nämlich diejenige, die die Mehrheitsgesellschaft im demokratischen Prozess als bindend anerkannt hat. Abweichende Kulturen, zum Beispiel ausländische Rechtsordnungen und Subkulturen bestehen aus rechtlicher Sicht zwar, ihnen kommt aber keine normativ bindende Wirkung zu. Sie berühren die durch das Recht normierte Kultur einerseits durch ihre faktischen Einwirkungen auf die Rechtsverwirklichung, andererseits bieten sie Ideen und Anschauungsmaterial für eine mögliche Modernisierung des geltenden Rechts. Eine globale Internetkultur ist aber nicht auf nationale rechtliche Kulturen beschränkt. Im Projekt wird daher

untersucht werden müssen, welche deutschen Kulturgüter rechtlich so abgesichert sind, dass sie auch in der Internetkultur zu beachten sind.

5.1.3 VERTRAUEN UND RECHT

Vertrauen bedeutet im Recht das Sichverlassen auf den Eintritt eines Ereignisses oder dessen Ausbleiben. Rechtserhebliches Vertrauen kann sich beziehen auf die Einhaltung von Gesetzen, Verträgen, besonderen Vertrauensverhältnissen, objektivrechtlichen Prinzipien, allgemeinen gesellschaftlichen Normen, auf das Eintreten anderen menschlichen Verhaltens oder das Eintreten von Zuständen. Vertrauen spielt an vielen Stellen im Recht eine Rolle. Das Recht knüpft einerseits Rechtsfolgen an Vertrauen und behandelt Vertrauen insofern als Voraussetzung. Andererseits bleibt das Recht nicht beim Vertrauen stehen, sondern enthält für viele Fälle des enttäuschten Vertrauens Durchsetzungsmechanismen oder zumindest Ausgleichs- und Ersatzansprüche, die ihrerseits durchgesetzt werden können und so das Vertrauen in die ursprüngliche Erwartung verstärken.[1004]

Tatsächliches Vertrauen als psychologische Disposition von Menschen lässt sich nicht wirksam anordnen, es kann aber durch rechtlich festgelegte Rahmenbedingungen gefördert werden. Hingegen können ein Vertrauen*dürfen* und Vertrauen*müssen* sehr wohl rechtlich angeordnet werden.

Rechtlich erhebliche oder rechtlich ausgestaltete Vertrauensverhältnisse kommen in personaler Hinsicht in drei Konstellationen vor. Entweder darf vertrauen oder hat zu vertrauen: ein Bürger einem anderen Bürger, ein Bürger dem Staat oder der Staat einem Bürger oder den Bürgern. Ein Bürger muss zum Beispiel bis zum Ablauf bestimmter Fristen darauf vertrauen, dass ein anderer Bürger den zwischen ihnen geschlossenen Kaufvertrag erfüllt. Ein Bürger muss zum Beispiel dem Staat außerhalb demokratischer Öffentlichkeitsgebote dahingehend vertrauen, dass dieser die Rechtsordnung achtet, und ihn vor Gefahren schützt. Der Staat muss den Bürgern dahingehend vertrauen, dass sie grundsätzlich die Gesetze achten und darf sie nicht generell überwachen. Im Hinblick auf ein Vertrauen im Internet wird zusätzlich das Vertrauen in technische Systeme erheblich.[1005]

Das rechtlich angeordnete Vertrauendürfen und Vertrauenmüssen schafft Räume zeitlicher, körperlicher oder erkenntnisstandsmäßiger Art, die verfolgungs- und vollstreckungsfrei sind. Entweder sind Fristen eingeräumt, die bis zur Rechtsverfolgung abgewartet werden müssen (wie zum Beispiel im Fall des Verzugs) oder es sind körperliche Räume festgelegt, in die die Einsicht in der Regel verwehrt ist (wie die Privatwohnung) oder es sind bestimmte Erkenntnisstände abzuwarten, bevor die Rechtsverfolgung einsetzen darf (wie zum Beispiel die Gefahrschwelle im Polizeirecht oder die Verdachtsstufen im Strafprozessrecht). Fahrlässigkeitsmaßstäbe regeln, inwiefern auf das Ausbleiben von Schäden vertraut werden darf, ohne dass dies einen Regress nach sich zieht. Durch diese rechtlich festgelegten Vertrauensräume wird eine Entlastung von Kontrolle geschaffen, sowohl für denjenigen, der ansonsten kontrolliert würde, als auch für denjenigen, der ansonsten kontrollieren müsste und bei dem durch das Vertrauen Ressourcen frei bleiben. Rechtlich regulierte Vertrauensräume schaffen oder erhalten dadurch auf beiden Seiten einen Handlungs- und Entfaltungsraum.

Bei der Förderung des tatsächlichen Vertrauens kann das Recht eine bedeutende Rolle spielen. Diese Wirkung hat schon die Rechtsordnung als allgemeiner Handlungsrahmen.[1006] Einzelne vertrauensfördernde Maßnahmen werden dann besonders wichtig, wenn herkömmliche

1004 Jandt 2008, S. 59.
1005 Zum Systemvertrauen Luhmann 2000, S. 26, 59 ff.
1006 Jandt 2008, S. 58.

Vertrauensanker wie der persönliche Kontakt nicht vorhanden sind. Zum Beispiel kann aufgrund der fehlenden persönlichen Begegnung im Internet fraglich sein, wer der Kommunikationspartner ist. Bei der Verarbeitung personenbezogener Daten in den Anwendungsszenarien kann unklar sein, wer die Daten verarbeitet und an wen sich die Betroffenen wenden müssen, wenn sie Auskunfts- oder Löschungsrechte ausüben möchten. Die Bezugsperson für das Vertrauen kann also unklar sein und damit die Frage bestehen, gegen wen sich eine eventuelle Rechtsverfolgung oder Rechtsdurchsetzung im Fall enttäuschten Vertrauens zu wenden hätte. Das Recht kann in einem solchen Fall Alternativmaßnahmen anordnen, die den fehlenden Vertrauensanker ersetzen sollen, wie zum Beispiel die Informationspflicht für Internetdienste gemäß § 5 Telemediengesetz. Weitere rechtliche Vertrauensanker können zum Beispiel Regresspflichten und insgesamt eine funktionierende Rechtsverfolgung und Rechtsdurchsetzung sein.[1007] Eine zentrale Rolle für eine *„Privatsphäre"* im Internet und ein *„Vertrauen"* in deren Bestehen nimmt die Ausgestaltung des Datenschutzrechts ein.[1008]

5.1.4 PRIVACY, PRIVATSPHÄRE UND GRUNDRECHTLICHE SCHUTZBEREICHE

Im deutschen Recht wird unter den Begriffen *„Privacy"* oder *„Privatsphäre"* kein einheitliches Schutzkonzept oder Rechtsgut verstanden. *„Privatsphäre"* ist vielmehr als Bezeichnung belegt für eine ganz bestimmte Schutzsphäre im Rahmen der Gewährleistung des allgemeinen Persönlichkeitsrechts (dazu sogleich). Auch wird die Bezeichnung auf EU-Ebene anders verwendet als im deutschen Recht. Die Bezeichnung eignet sich daher nicht, um den rechtlichen Schutz des Phänomens zu beschreiben, das im Projekttitel, in der Fachsprache anderer Disziplinen oder in der Umgangssprache als *„Privatsphäre"* bezeichnet wird.

5.2 RECHTLICHE SCHUTZGÜTER EINER *„KULTUR DER PRIVATSPHÄRE UND DES VERTRAUENS IM INTERNET"*

Der rechtliche Schutz muss vielmehr beschrieben werden durch die nun folgende Darlegung der einzelnen rechtlichen Schutzgüter, die das gesellschaftliche Phänomen *„Privatsphäre"* in seinen unterschiedlichen Facetten schützen und die insofern von Risiken in den Anwendungsszenarien betroffen sein können. Betrachtet werden aber auch Grundrechte, die durch die Nutzung der Internetdienste der Anwendungsszenarien in ihrer Verwirklichung gefördert werden, wie zum Beispiel die Informations- und Meinungsfreiheit oder die Berufsfreiheit. So kann dargestellt werden, welche Rechtspositionen sich hier gegenüberstehen und zum Ausgleich gebracht werden müssen.

5.2.1 VERFASSUNGSRECHTLICHE SCHUTZGÜTER

5.2.1.1 Allgemeines Persönlichkeitsrecht

Das allgemeine Persönlichkeitsrecht wird aus der freien Entfaltung der Persönlichkeit aus Art. 2 Abs. 1 GG in Verbindung mit der Menschenwürde aus Art. 1 Abs. 1 GG hergeleitet. Schutzgegenstand des allgemeinen Persönlichkeitsrechts sind sowohl die Selbstfindung im abgeschirmten Privatbereich als auch die Selbstdarstellung in der Öffentlichkeit.[1009] Als lückenschließendes Auffanggrundrecht schützt das allgemeine Persönlichkeitsrecht jede Art von Betätigungen, sodass es überall dort greift, wo kein spezielleres Grundrecht einschlägig ist.[1010]

Für die gemäß Art. 2 Abs. 1 GG grundsätzlich gegebene Einschränkbarkeit des allgemeinen Persönlichkeitsrechts durch förmliche Gesetze wird vom Bundesverfassungsgericht danach unterschieden, ob die Einschränkung die *„Intimsphäre"*, die *„Privatsphäre" oder die „Sozialsphäre"* betrifft.

1007 Jandt 2008, S. 52 ff.
1008 Jandt 2008, S. 71.
1009 Dreier, in: Dreier 2004, Art. 2 Abs. 1 GG, Rn. 24.
1010 Siehe zum Beispiel Dreier, in: Dreier 2004, Art. 2 Abs. 1 GG, Rn. 30.

Die Intimsphäre (auch *„Kernbereich privater Lebensgestaltung"*) genießt einen absoluten Schutz. Eingriffe in diesen Bereich sind nicht zu rechtfertigen. Den geringsten Schutz genießt die Sozialsphäre. Die Persönlichkeit wird dort als Teil der sozialen Realität in der Öffentlichkeit der sozialen Gemeinschaft entfaltet. Betroffene müssen in diesem Bereich Einschränkungen hinnehmen, wenn und soweit diese durch Gründe des Gemeinwohls oder überwiegende Rechtsinteressen Dritter getragen werden.[1011] Zwischen diesen beiden liegt die *„Privatsphäre"*, die der Einzelne der Öffentlichkeit verschließt und nur ausgewählten Vertrauten öffnet. In diesen Bereich darf nur unter strenger Wahrung des Verhältnismäßigkeitsgrundsatzes eingegriffen werden.[1012] Bezüglich der automatisierten Datenverarbeitung wurde die Sphärentheorie allerdings aufgegeben. Der Schutz kann hier nicht von der Sphäre abhängen, aus der die Daten stammen, sondern muss die Verwendbarkeit der Daten berücksichtigen. Aufgrund der Vielzahl von Informationen, die mit Hilfe der automatisierten Datenverarbeitung aus dem Zusammenspiel einzelner, nicht intimer Daten gezogen werden könnten, gibt es „kein belangloses Datum".[1013]

Das allgemeine Persönlichkeitsrecht ist wie alle Freiheitsrechte zunächst ein gegen staatliche Eingriffe gerichtetes Abwehrrecht. Darüber hinaus trifft den Staat aber auch eine Pflicht, sich schützend und fördernd vor das Grundrecht zu stellen. Aufgrund dieser Schutzpflicht muss er Übergriffen anderer Privater durch gesetzliche Sanktionen entgegenwirken.[1014]

Das Bundesverfassungsgericht hat das allgemeine Persönlichkeitsrecht durch mehrere, nicht ausdrücklich im Grundgesetz enthaltene Konkretisierungen ausgeformt konkretisiert, die für den informationstechnischen Bereich relevant sind. Sie werden im Folgenden dargestellt.

Recht auf informationelle Selbstbestimmung

Als Konkretisierung des allgemeinen Persönlichkeitsrechts aus Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG wurde das Recht auf informationelle Selbstbestimmung vom Bundesverfassungsgericht in seinem Volkszählungsurteil[1015] bereits im Jahre 1983 entwickelt. „Individuelle Selbstbestimmung setzt" für das Bundesverfassungsgericht „voraus, dass dem Einzelnen Entscheidungsfreiheit über vorzunehmende oder zu unterlassende Handlungen einschließlich der Möglichkeit gegeben ist, sich auch entsprechend dieser Entscheidung tatsächlich zu verhalten". Wer (aber) „nicht mit hinreichender Sicherheit überschauen kann, welche ihn betreffenden Informationen in bestimmten Bereichen seiner sozialen Umwelt bekannt sind, und wer das Wissen möglicher Kommunikationspartner nicht einigermaßen abzuschätzen vermag, kann in seiner Freiheit wesentlich gehemmt werden, aus eigener Selbstbestimmung zu planen oder zu entscheiden."[1016]

Als die verfassungsrechtliche Antwort auf „die modernen Bedingungen der Datenverarbeitung" hat das Bundesverfassungsgericht daher die informationelle Selbstbestimmung als Grundrecht anerkannt. „Das Grundrecht gewährleistet die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen."[1017] Die informationelle Selbstbestimmung ist – neben der Informationsfreiheit und dem Telekommunikationsgeheimnis – das zentrale Grundrecht der Informationsgesellschaft.[1018] Sie hat eine subjektive und eine objektive Schutzrichtung.[1019]

1011 Siehe zum Beispiel BVerfGE 35, 202 (220 f.).
1012 Starck, in: Mangoldt / Klein / Starck 2010, Art. 2 Abs. 1 GG, Rn. 173.
1013 Siehe zum Beispiel BVerfGE 65, 1 (45).
1014 Siehe zum Beispiel Dreier, in: Dreier 2004, Art. 2 Abs. 1 GG, Rn. 89.
1015 Siehe zum Beispiel BVerfGE 65, 1.
1016 BVerfGE 65, 1 (43).
1017 BVerfGE 65, 1 (43).
1018 Siehe näher Trute, in: Roßnagel 2003, S. 156 ff.
1019 Siehe zum Folgenden Roßnagel 2008, S. 132 f.

Die informationelle Selbstbestimmung schützt einmal die selbstbestimmte Entwicklung und Entfaltung des Einzelnen. Seine Persönlichkeit wird geprägt durch das Gesamtbild des Handelns und Kommunizierens in unterschiedlichen sozialen Rollen. Sie setzt für ihre Entfaltung voraus, dass er sich in diesen Rollen darstellen kann und ihm diese Selbstdarstellung in der Kommunikation mit anderen zurückgespiegelt wird. Individuelle Entwicklung und Entfaltung kann nur gelingen, wenn der Betroffene die Preisgabe von Angaben über sich kontrollieren kann. Kann er diese aber nicht erkennen, kann er „in seiner Freiheit wesentlich gehemmt werden, aus eigener Selbstbestimmung zu planen oder zu entscheiden". Dementsprechend muss der Einzelne in der Lage sein, selbst zu entscheiden, welche Daten er über sich in welcher Rolle und in welcher Kommunikation preisgibt. Diesen Vorrang autonomer Entscheidung über Informationsfreigaben schützt das Grundrecht auf informationelle Selbstbestimmung.

In dieses Grundrecht greift derjenige ein, der Daten der betroffenen Person gegen ihren Willen verarbeitet – unabhängig davon, ob dies eine staatliche Behörde oder ein privates Unternehmen ist. Die betroffene Person ist in beiden Fällen gleich schutzwürdig. Die Missachtung ihrer informationellen Selbstbestimmung ist in beiden Fällen ein Grundrechtseingriff.[1020] Allerdings begründet das Grundrecht nur gegenüber der staatlichen Gewalt eine unmittelbare Abwehrfunktion. Für private Unternehmen ist zu berücksichtigen, dass sie sich ebenfalls auf Grundrechte – hier vor allem die Freiheit der Berufsausübung – berufen können. Allerdings ermächtigen die Grundrechte nicht dazu, in andere Grundrechte einzugreifen. Vielmehr ist es Aufgabe des Gesetzgebers, konkurrierende Grundrechtssphären so abzugrenzen, dass die Ausübung von Grundrechten nicht dazu führt, dass dadurch in die Grundrechte anderer eingegriffen wird. Soweit der Gesetzgeber nicht das Grundrecht auf informationelle Selbstbestimmung zugunsten überwiegender privater Interessen durch Gesetz eingeschränkt hat, haben Private kein eigenständiges Recht zur Verarbeitung personenbezogener Daten Dritter.[1021]

Informationelle Selbstbestimmung ist nicht nur ein subjektives Recht des jeweils Betroffenen, sondern zugleich auch die Grundlage einer freien und demokratischen Kommunikationsverfassung.

> „Mit dem Recht auf informationelle Selbstbestimmung wäre eine Gesellschaftsordnung und eine diese ermöglichende Rechtsordnung nicht vereinbar, in der Bürger nicht mehr wissen können, wer was wann und bei welcher Gelegenheit über sie weiß. ... Dies würde nicht nur die individuellen Entfaltungschancen des Einzelnen beeinträchtigen, sondern auch das Gemeinwohl, weil Selbstbestimmung eine elementare Funktionsbedingung eines auf Handlungs- und Mitwirkungsfähigkeit seiner Bürger begründeten freiheitlich demokratischen Gemeinwesens ist."[1022]

> „Das Grundrecht dient dabei auch dem Schutz vor einem Einschüchterungseffekt, der entstehen und zu Beeinträchtigungen bei der Ausübung anderer Grundrechte führen kann, wenn für den Einzelnen nicht mehr erkennbar ist, wer was wann und bei welcher Gelegenheit über ihn weiß."[1023]

Informationelle Selbstbestimmung zielt somit auf eine Kommunikationsordnung, die einen selbstbestimmten Informationsaustausch und eine freie demokratische Willensbildung ermöglicht.

In dieser überindividuellen Funktion ist die informationelle Selbstbestimmung auch Element einer „objektiven Wertordnung", „die als verfassungsrechtliche Grundentscheidung für alle Bereiche des Rechts gilt und Richtlinien und Impulse

1020 BVerfGE 84, 192 (195).
1021 Siehe zum Beispiel Roßnagel / Pfitzmann / Garstka 2001, S. 46 ff.
1022 BVerfGE 65, 1 (43); BVerfG, NJW 2006, 976 (979), Rn. 87.
1023 BVerfG, NJW 2006, 976 (979), Rn. 86.

für Gesetzgebung, Verwaltung und Rechtsprechung gibt".[1024] Sie und die anderen Grundrechte bilden zentrale Grundpfeiler einer freien gesellschaftlichen Ordnung. Sie sind bei der Interpretation aller Rechtsnormen zu beachten und füllen vor allem die inhaltlich offenen Normen des Privatrechts aus.

Informationelle Selbstbestimmung begründet daher kein eigentumsähnliches Herrschaftsrecht über personenbezogene Daten. Sie ist als Funktionsvoraussetzung einer freien und demokratischen Gesellschaft nicht in das – vom richtigen Preis abhängige – Belieben des Individuums als Händler seiner Daten gestellt. Ein solches Missverständnis würde auch dem Charakter personenbezogener Daten als mehrrelationales Modell der Wirklichkeit nicht gerecht. So „gehören" – etwa im Beispiel des Ubiquitous Computing im Straßenverkehr – Wartungsdaten eines Kraftfahrzeugs nicht nur dessen Eigentümer, sondern auch dem Reparaturbetrieb. Eine ausschließliche Zuordnung zu einem – dem Autor oder dem Objekt des Wirklichkeitsmodells *„Wartung des Autos"* – ist nicht möglich.[1025] Vielmehr ist eine Informations- und Kommunikationsordnung gefragt, die bestimmt, wer in welcher Beziehung befugt ist, mit dem Modell in einer bestimmten Weise umzugehen. Diese Ordnung soll Kommunikation nicht unterbinden, sondern – allerdings selbstbestimmt – ermöglichen. Datenschutz bezweckt nicht den Schutz des Eigenbrötlers, der sich von der Welt abschotten will,[1026] sondern den Schutz des selbstbestimmt in der Gesellschaft Agierenden und Kommunizierenden. Gesellschaftliche Einbindung aber setzt Kommunikation voraus und verpflichtet zu Kommunikation und damit in bestimmten Situationen auch zur Preisgabe personenbezogener Daten. Soweit überwiegende Allgemein- oder Individualinteressen es erfordern, ist auch eine Datenverarbeitung gegen den Willen des Betroffenen möglich. Diese Situationen zu bestimmen und zu regeln, ist Aufgabe des Datenschutzrechts.

Computergrundrecht

Da Computer für die Persönlichkeitsentfaltung in einer Informationsgesellschaft von erheblicher Bedeutung geworden sind, hat das Bundesverfassungsgericht aus dem allgemeinen Persönlichkeitsrecht des Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG das sogenannte Computergrundrecht entwickelt. Das Computergrundrecht soll die Vertraulichkeit und Integrität informationstechnischer Systeme gewährleisten, insbesondere von mobilen und immobilen Personalcomputern, Mobiltelefonen und elektronischen Terminkalendern.[1027]

Vertraulichkeit schützt das Vertrauen in das Geheimbleiben der durch das informationstechnische System erzeugten Daten; Integrität schützt das Vertrauen des Nutzers in die Sicherheit des Systems. Er darf darauf vertrauen, dass dieses nicht von außen infiltriert und die entstandenen Daten nicht ausgespäht werden und dass weder die Daten noch die Funktionen des Systems verändert werden. Das Computergrundrecht schützt vor staatlichen Eingriffen in informationstechnische Systeme und vor Erhebung der Daten (Online-Durchsuchung), sofern nicht andere Grundrechte, insbesondere die informationelle Selbstbestimmung aus Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG und das Fernmeldegeheimnis aus Art. 10 Abs. 1 GG vorrangig sind. Eingriffe können nach dem Urteil des Bundesverfassungsgerichts gerechtfertigt sein, sofern sie präventiven Maßnahmen oder Strafverfolgungszwecken dienen und dem Verhältnismäßigkeitsgebot genügen, also nach Abwägung der betroffenen Rechtsgüter erforderlich und angemessen sind.

Das Recht auf Vertraulichkeit und Integrität informationstechnischer Systeme gewährleistet ein Abwehrrecht gegenüber staatlichen Einrichtungen sowie ein Schutzrecht gegenüber dem Gesetzgeber auf Sicherstellung der Vertraulichkeit

1024 BVerfGE 39, 1 (41) - Hervorhebung durch die Verfasser.
1025 BVerfGE 65, 1 (44).
1026 Hier unterscheidet sich die amerikanische Privacy als *„right to be let alone"* vom europäischen Konzept der informationellen Selbstbestimmung.
1027 Siehe zum Beispiel BVerfGE 120, 274 (314).

und Integrität solcher Systeme gegenüber Privaten, da die Gefährdungen der informationstechnischen Systeme nicht nur durch den Staat entstehen, sondern auch durch Private.

Das Recht am eigenen Wort und das Recht am eigenen Bild

Die Recht am eigenen Wort und am eigenen Bild sind ebenfalls Konkretisierungen des allgemeinen Persönlichkeitsrechts aus Art. 2 Abs. 1 und Art. 1 Abs. 1 GG.

Das Recht am eigenen Wort[1028] umfasst den Schutz des nicht öffentlich gesprochenen Wortes sowie schriftlicher Aufzeichnungen unabhängig vom Medium. Es schützt auch vor Falschzitaten und erdachten Interviews. Einfachgesetzlich ist es zum Beispiel durch die Strafnorm des § 201 STGB geschützt.

Das Recht am eigenen Bild[1029] schützt vor heimlichen oder erzwungenen bildlichen Aufnahmen einer Person in jedweder Form (auch Web-Cam-Aufnahmen) sowie deren Verbreitung. Grundrechtsadressat ist zunächst die öffentliche Gewalt. Die hieraus resultierende Schutzpflicht des Staates schlägt sich in der einfachgesetzlichen Verankerung dieses Rechtes nieder: Gegenüber Privaten ist das Recht am eigenen Bild durch §§ 22 ff. KunstUrhG geschützt. Danach ist zur Veröffentlichung von Bildnissen eine Einwilligung des Abgebildeten erforderlich, die nur unter engen Voraussetzungen entbehrlich ist. Strafrechtlich wird dieses Recht durch § 201a StGB geschützt.

5.2.1.2 Fernmeldegeheimnis

Das Fernmeldegeheimnis in Art. 10 GG schützt das Vertrauen des Einzelnen, dass ein individueller Kommunikationsvorgang mit fernmeldetechnischen Anlagen nicht von Dritten zur Kenntnis genommen wird. Davon umfasst sind insbesondere nicht-körperliche Kommunikationsvorgänge wie Telefax, E-Mails, Skype, Mitteilungen über soziale Netzwerke oder Instant Messaging Dienste.[1030] Der Schutzbereich umfasst sowohl die Umstände (zum Beispiel ob, wann, wie lange, zwischen welchen Anschlüssen/Personen) als auch den Inhalt (Vertraulichkeit der Information).[1031]

Kommunikation in diesem Sinne meint ausschließlich die nichtöffentliche Kommunikation mit einem begrenzten, individualisierten Empfängerkreis.[1032] Nur dann besteht überhaupt ein berechtigtes Geheimhaltungsinteresse. Der Vorgang muss also durch technische Mittel vor einem allgemein öffentlichen Zugang geschützt werden, sei es durch Passwort oder Verschlüsselung und durch vorherige Festlegung des Empfängerkreises. Die Abgrenzung ist indes vielfach schwierig und bedarf immer einer Einzelfallbetrachtung.[1033] In den Schutzbereich fallen nicht Rundfunk und Webradio sowie alle Formen der öffentlichen Kommunikation[1034] wie Äußerungen auf öffentlich zugänglichen, nicht zugangsbeschränkten Plattformen (Leser-/Kundenkommentare oder Ähnliches).

Unerheblich ist, ob eine Abhörmaßnahme an der Übertragungsstrecke oder am Endgerät (zum Beispiel Laptop, Handy, PDA, PC) ansetzt,[1035] der Kommunikationsvorgang darf jedoch nicht abgeschlossen sein. Nicht geschützt ist das Vertrauen der Kommunikationspartner untereinander. Ein Vorgang fällt nur unter den Schutz von Art. 10 GG, wenn staatliche Ermittlungsmaßnahmen von außen, also nicht als Partner der Kommunikation durchgeführt werden. Art. 10 GG begründet somit zum einen ein Abwehrrecht[1036] gegenüber Staatsorganen. Es untersagt Beeinträchtigungen von

1028 Siehe zum Beispiel BVerfGE 34, 238 (246 ff.).
1029 Siehe zum Beispiel BVerfGE 35, 202 (220).
1030 Siehe zum Beispiel Gusy, in: Mangoldt / Klein / Starck 2010, Art. 10 GG, Rn. 39.
1031 Siehe zum Beispiel BVerfGE 67, 157 (172) – G 10; 85 (386, 396) – Fangschaltungen.
1032 Siehe zum Beispiel Gusy, in: Mangoldt / Klein / Starck 2010, Art. 10 GG, Rn. 39, 42, 44.
1033 Genauer hierzu Ohly, AfP 2011, S. 428.
1034 Siehe zum Beispiel Gusy, in: Mangoldt / Klein / Starck 2010, Art. 10 GG, Rn. 44.
1035 Siehe zum Beispiel BVerfGE 120, 274 (307).
1036 Gusy, in: v. Mangoldt / Klein / Starck 2010, Art. 10 GG, Rn. 57.

Schutzvorkehrungen zur Vertraulichkeit der Kommunikation wie technische Möglichkeiten zur Überwachung des Fernmeldeverkehrs,[1037] Speicherung geschützter Informationen zur späteren Verwendung (Vorratsdatenspeicherung) sowie Kenntnisnahme, Aufzeichnung und Registrierung geschützter Informationen, insbesondere Verbindungsdaten. Da der Staat nicht (mehr) Betreiber der Netze ist, trifft ihn aber auch eine Schutz- und Abwehrpflicht, durch Regulierung die Einhaltung der Grundrechte sicherzustellen.[1038]

Ein Eingriff in das Fernmeldegeheimnis (Kenntnisnahme, Speicherung und Verwendung oder Weitergabe an Dritte) bedarf einer gesetzlichen Grundlage und muss insbesondere verhältnismäßig sein.

5.2.1.3 Unverletzlichkeit der Wohnung

Schutzgut des Art. 13 Abs. 1 GG ist die räumliche Sphäre, in der sich das Privatleben entfaltet. Dies ist nicht beschränkt auf Privatwohnungen,[1039] vielmehr sind auch Betriebs- und Geschäftsräume[1040] umfasst sowie jeder dem Schutz der Privatheit gewidmete Raum, da zur freien Entfaltung der Persönlichkeit ein elementarer Lebensraum erforderlich ist.[1041]

Als Grundrechtsträger genießt jedermann Schutz vor unbefugtem physischem Eindringen in die Wohnung, Einschleusen von Spionageprogrammen (Online-Durchsuchung), wenn hierfür in die Wohnung eingedrungen wird,[1042] vor akustischer und optischer Wohnraumüberwachung[1043] (Lauschangriff) sowie vor Messung elektromagnetischer Strahlungen, mit der die Nutzung eines informationstechnischen Systems nachgewiesen werden kann, auch wenn dieses nicht online arbeitet.[1044] Art. 13 Abs. 1 GG ist auch dann berührt, wenn die Hardware des PCs (zum Beispiel die Web-Cam) ferngesteuert und zur Wohnraumüberwachung genutzt wird.[1045] Zugriffe auf E-Mails, die auf dem Server des Providers gespeichert sind, unterliegen mangels räumlicher Nähe nicht dem Schutz des Art. 13 Abs. 1 GG.[1046] Art. 13 Abs. 1 GG schützt nicht vor der Erhebung von Daten auf dem Speichermedium schlechthin, da das informationstechnische System standortunabhängig eingesetzt werden kann (insbesondere Laptops, PDAs und Mobiltelefone) und deshalb der allein räumliche Schutz des Art. 13 Abs. 1 GG nicht weiterhilft.[1047]

Art. 13 Abs. 1 GG bindet in erster Linie Gesetzgeber und Rechtsprechung und begründet Schutzpflichten zur gesetzlichen Sicherstellung des Grundrechts auch gegenüber Privaten.

5.2.1.4 Meinungs- und Informationsfreiheit

Die Meinungsfreiheit des Art. 5 Abs. 1 GG umfasst die Meinungsbildungs-, Meinungsäußerungs- und die Meinungsverbreitungsfreiheit. Eine Meinung ist eine subjektive Wertung zu allen denkbaren sachlichen und personellen, öffentlichen oder privaten Gegenständen und Angelegenheiten, unerheblich, ob sie von grundsätzlicher Bedeutung, wertvoll, falsch oder allgemeingültig ist.[1048] Medien zur Meinungskundgabe sind das gesprochene Wort, Schrift, auch die elektronische Kundgabe im Internet sowie Bilder (alle bildlichen Darstellungen, die nicht Schrift sind: Symbole, Zeichnungen, Farben und Farbkombinationen).

1037 Siehe zum Beispiel BVerfGE 67, 157 (180).
1038 Ausführlicher hierzu Gusy, in: Mangoldt / Klein / Starck 2010, Art. 10 GG, Rn. 63 f.
1039 Siehe zum Beispiel BVerfGE 89, 1 (12).
1040 Siehe zum Beispiel BVerfGE 32 (54).
1041 Siehe zum Beispiel BVerfGE 42, 212 (219).
1042 Gornig, in: Mangoldt / Klein / Starck 2010, Art 13 GG, Rn. 43.
1043 Siehe zum Beispiel BVerfGE 109, 279 (309, 327) – Großer Lauschangriff; BVerfGE 120, 274 (310).
1044 Siehe zum Beispiel BVerfGE 120, 274, (310).
1045 Siehe zum Beispiel BVerfGE 120, 274 (310).
1046 Die Beschlagnahme von E-Mails ist gemäß BVerfGE 124, 43 an Art. 10 GG zu messen.
1047 Siehe zum Beispiel BVerfGE 120, 274 (311).
1048 Siehe zum Beispiel BVerfGE 33, 1 (15); Starck, in: Mangoldt / Klein / Starck 2010, Art. 5 GG, Rn. 22.

Die ebenfalls in Art. 5 Abs. 1 GG verankerte Informationsfreiheit schützt das Recht, sich aus allgemein zugänglichen Quellen, wie dem offenen Internet, ungehindert zu unterrichten.

Das Internet hält insgesamt ein hohes förderliches Potential für die Verwirklichung der Meinungs- und Informationsfreiheit bereit. Fehlende Sicherheit, Integrität und Vertrauen in die Privatheit des Internets können aber abschreckend auf eine Meinungsäußerung im Internet wirken und damit zu einer Anpassung des Verhaltens durch den Nutzer und bei Meinungsäußerungen womöglich zu einer Selbstzensur führen.[1049]

5.2.1.5 Berufsfreiheit und Recht am eingerichteten und ausgeübten Gewerbebetrieb

Die Berufsfreiheit des Art. 12 Abs. 1 GG umfasst neben der Berufswahlfreiheit auch die Berufsausübungsfreiheit.[1050] Daneben wird auch vertreten, dass ein Recht am eingerichteten und ausgeübten Gewerbebetrieb als Unterfall des Eigentumsgrundrechts des Art. 14 GG anzuerkennen sei. Dieses soll die Sach- und Rechtsgesamtheit des wirtschaftlichen Unternehmens schützen.[1051] Viele Wirtschaftszweige profitieren vom Sammeln und Weitergeben personenbezogener Daten (Auskunfteien, Werbung, Adresshandel, Marktforschung). Das Internet hat hier zu einer Vervielfältigung der unternehmerischen Möglichkeiten geführt (größere Zielgruppen, gezielteres Anwerben, Unabhängigkeit von Standortfaktoren). In nicht unerheblichem Maße setzt dies gerade die Erhebung und Verarbeitung von Nutzerdaten voraus, um Einblicke in das Nutzerverhalten sowie die Interessen und Vorlieben potenzieller Kunden zu gewinnen.

5.2.1.6 Grundrechtsabwägung

Die Grundrechte und die Grundrechtsträger können zueinander in Konflikt geraten. Solche Konflikte können insbesondere dadurch entstehen, dass das Sammeln von Daten durch Unternehmen auf der einen Seite Ausfluss der Grundrechte auf Berufsausübung und auf unternehmerische Handlungsfreiheit ist, auf der anderen Seite aber in die Grundrechte auf informationelle Selbstbestimmung und die übrigen *„Privatheitsrechte"* eingreift. Diese Grundrechtskonflikte sind nach dem Prinzip der praktischen Konkordanz auszugleichen: Es muss nach Gestaltungen der Geschäftsmodelle und Ablaufprozesse gesucht werden, die möglichst viel an Verwirklichung der konfligierenden Interessen auf beiden Seiten ermöglicht.

5.2.2 EUROPÄISCHE FREIHEITSRECHTE

Grundrechte auf europäischer Ebene finden sich in der europäischen Menschenrechtskonvention (EMRK) sowie in der Charta der Grundrechte der Europäischen Union (EGRC). Art. 6 Abs. 1 EUV erklärt die Grundrechtecharta gleichrangig mit den Primärverträgen (EUV und AEUV) und damit für unmittelbar anwendbar und verbindlich. Gemäß Art. 6 Abs. 2 des Vertrages über die Europäische Union (EUV) tritt die Union als Völkerrechtssubjekt der Menschenrechtskonvention bei und verpflichtet sich damit zur Einhaltung der Menschenrechte. Beide Regelwerke sehen Grundrechte ähnlich wie die im Grundgesetz Niedergelegten vor.

5.2.2.1 EU-Grundrechtecharta

Art. 8 EGRC gewährleistet den Schutz personenbezogener Daten und regelt Umfang und Grenzen der Verarbeitung. Ziel ist die Verwirklichung des freien Verkehrs personenbezogener Daten im Binnenmarkt auf einem hohen Niveau des Datenschutzes. Art. 8 EGRC ist *lex specialis* zu Art. 7 EGRC (Achtung des Privatlebens) und geht diesem daher vor. Umgesetzt wird der Schutzauftrag für das Grundrecht durch die EU-Datenschutzrichtlinie 95/46/EG und die Richtlinie für den Datenschutz in der elektronischen Kommunikation 2002/58/EG. Umfasst werden personenbezogene

1049 Dazu auch BGHZ 181 (328-345) – Spickmich.de.
1050 Siehe zum Beispiel Manssen, in Mangoldt / Klein / Starck 2010, Art. 12 GG, Rn. 1 und 5.
1051 Siehe zum Beispiel Depenheuer, in Mangoldt / Klein / Starck 2010, Art. 14 GG, Rn. 132; das BVerfG hat es offengelassen, ob ein solches Grundrecht besteht.

Daten.[1052] Der sachliche Anwendungsbereich wird mit *„Verarbeitung"* umschrieben.[1053] Dieser Begriff umfasst – anders als im Bundesdatenschutzgesetz – alle Formen des Umgangs mit personenbezogenen Daten. Berechtigt sind neben natürlichen Personen über die Richtlinie 2002/58/EG für den Bereich der elektronischen Kommunikation auch juristische Personen. Verpflichtet ist neben den Mitgliedsstaaten auch die Union selbst (VO (EG) Nr. 45/2001).

Die Verarbeitung personenbezogener Daten darf gemäß Art. 8 Abs. 2 EGRC nur zweckgebunden erfolgen. Liegt keine Einwilligung der betroffenen Person vor, ist die Verarbeitung nur zulässig, wenn sie auf gesetzlicher Grundlage zum Zwecke übergeordneter Interessen (Erfüllung eines bindenden Vertrags, Wahrung lebenswichtiger Interessen, Erfüllung rechtlicher Verpflichtungen, öffentliches Interesse) erforderlich ist.[1054] Der europäische Gesetzgeber hat durch die entsprechenden Rechtsakte (Verordnung, Richtlinie) die Durchsetzung des Datenschutzes durch EU-Behörden und Mitgliedsstaaten sicherzustellen. Ein Verstoß gegen Art. 8 EGRC kann gerichtlich gemäß Art. 47 Abs. 2 EGRC geltend gemacht werden.

Die Grundrechtecharta entfaltet gemäß Art. 51 Abs. 1 EGRC Geltung für alle Unionsorgane und für die Mitgliedsstaaten bei Anwendung des Unionsrechts. Jede Einschränkung der in der Charta enthaltenen Grundrechte muss gemäß Art. 52 Abs. 1 EGRC durch Gesetz erfolgen und den Grundsatz der Verhältnismäßigkeit wahren.

5.2.2.2 Vertrag über die Arbeitsweise der Europäischen Union (AEUV)

Art. 16 AEUV wurde durch den Vertrag von Lissabon neu in die Primärverträge aufgenommen. Abs. 1 garantiert ein Grundrecht auf Datenschutz, während Abs. 2 als Kompetenz ausgestaltet ist, zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten Rechtsregeln zu erlassen. Die Union ist somit umfassend an das Grundrecht gebunden. Art. 16 Abs. 1 gilt ebenfalls nicht schrankenlos.[1055] Einschränkungen sind wie bei Art. 8 EGRC zulässig.

5.2.2.3 Europäische Menschenrechtskonvention

Die EMRK garantiert in Art. 8 ein Recht auf Achtung des Privatlebens, das das Brief- und Fernmeldegeheimnis mit umfasst. Inhaltlich besteht kein Unterschied zu den bereits vorgestellten deutschen Grundrechten.

5.3 AKTUELLE UND ABSEHBARE CHANCEN UND RISIKEN FÜR DIE RECHTLICHEN SCHUTZGÜTER

In diesem Abschnitt werden die wesentlichen aktuellen und absehbaren Chancen und Risiken in den Anwendungsszenarien auf die dargestellten Rechtsgüter bezogen, um zu zeigen, inwiefern sie die dargestellten Rechtsgüter betreffen.

5.3.1 PERSONALIZED WEB UND E-COMMERCE-DIENSTE

Personalisierte Internetdienste wie Suchmaschinen und E-Commerce-Angebote bieten sowohl auf Nutzer- als auch auf Anbieterseite Chancen für die Verwirklichung rechtlich geschützter Güter. So kann zum Beispiel eine personalisierte Ergebnisliste einer Suchmaschine die Informationsfreiheit des Suchenden aus Art. 5 Abs. 1 GG fördern. Den Anbietern der Dienste ermöglicht die Personalisierung der Dienste eine genauere und effizientere Diensterbringung. Überdies können sie Werbung passgenauer platzieren, Kundenwünsche analysieren und mit diesen Daten Handel treiben. Diese unternehmerischen Interessen können durch die Berufsfreiheit aus Art. 12 Abs. 1 GG und das

1052 Nur Daten mit Binnenmarktrelevanz, im Ergebnis aber Schutz darüber hinaus gehend (unter Bezugnahme auf die Rechtstexte des Europarates), Bernsdorff, in: Meyer 2011, Art. 8 EGRC, Rn. 15.
1053 Vergleiche die Begriffsbestimmung in Art. 2 lit. b) 95/46/EG.
1054 Art. 7 der Richtlinie 95/46/EG.
1055 Siehe zum Beispiel Kingreen, in: Callies / Ruffert 2011, Art. 16 AEUV, Rn. 3, 4.

Recht am eingerichteten und ausgeübten Gewerbebetrieb aus Art. 14 Abs. 1 GG geschützt sein.

Die Datenerhebung im Rahmen der angesprochenen Dienste birgt allerdings auch erhebliche Risiken für die informationelle Selbstbestimmung und das Computergrundrecht aus Art. 2 Abs. 1 und Art. 1 Abs. 1 GG sowie für das Fernmeldegeheimnis aus Art. 10 Abs. 1 GG. Durch die Personalisierung können verschiedenste Persönlichkeitsprofile erstellt werden, wie zum Beispiel Suchhistorien, Surfverhalten, Einkaufsverhalten und daraus auf politische Interessen, Gesundheitsprobleme, sexuelle Vorlieben, weltanschauliche Einstellungen, religiöse Überzeugungen und vieles mehr geschlossen werden. Das Ablegen von Cookies gefährdet die Integrität der privaten Endgeräte, das Auslesen von Browser- und OS-Fingerprints ihre Vertraulichkeit. Die Daten können überdies auf Vorrat vorgehalten werden, um zu immer neuen Zwecken ausgewertet zu werden. Die personenbezogenen Datenverarbeitungen im Rahmen von Suchmaschinen und E-Commerce werden zudem regelmäßig ohne Kenntnis der Nutzer vorgenommen, sodass von einem selbstbestimmten Umgang mit den personenbezogenen Daten häufig nicht die Rede sein kann. Die Nutzer haben kaum einen Überblick darüber, welche Daten von wem wie lange gespeichert werden und an wen sie möglicherweise übermittelt werden und damit, wem gegenüber sie Rechtsschutz zu suchen hätten.

Aufgrund der möglichen und intendierten Profilbildung, der potentiellen besonderen Sensitivität der Daten, der möglichen Vorratsspeicherung für noch unbestimmte Zwecke und der weitgehend unbemerkten Verarbeitung bringen die personalisierten Internetdienste und der E-Commerce hohe Risiken für die betroffenen Grundrechte mit sich.

5.3.2 SOZIALE NETZWERKE

Die Erhebung und Weiterverarbeitung personenbezogener Daten im Rahmen der Nutzung sozialer Netzwerke hat förderliche Auswirkungen auf die Verwirklichung bestimmter Grundrechte. Die Meinungs- und Informationsfreiheit aus Art. 5 Abs. 1 GG werden durch den erhöhten Kommunikationsaustausch einer Vielzahl von global verteilten Menschen, die ohne die Netzwerke vermutlich nicht in Kontakt getreten wären, erheblich gefördert. Überdies können die sozialen Netzwerke den Nutzern dabei helfen, sich und ihre berufliche Qualifikation einem breiten oder einem gezielt ausgewählten Interessentenkreis zu präsentieren und damit die Berufsfreiheit aus Art. 12 Abs. 1 GG fördern. Für Unternehmen ergeben sich neue Geschäftsmodelle und Rekrutierungsmöglichkeiten. Sie können durch die Auswertung der Daten Werbung erfolgreicher platzieren, Kundenwünsche analysieren und geeignete Mitarbeiter finden. Diese unternehmerischen Anliegen können durch die nach Art. 12 Abs. 1 und Art. 14 Abs. 1 GG geschützte unternehmerische Freiheit gedeckt sein. Auch für die nach Art. 5 Abs. 3 GG geschützte Wissenschaft können die Daten aus sozialen Netzwerken sehr wertvoll sein.

Aus der Erhebung und Verarbeitung personenbezogener Daten im Rahmen sozialer Netzwerke ergeben sich aber auch erhebliche Risiken für die informationelle Selbstbestimmung aus Art. 2 Abs. 1 und Art. 1 Abs. 1 GG und das Fernmeldegeheimnis aus Art. 10 Abs. 1 GG. Die Nutzer nutzen soziale Netzwerke zwar freiwillig. Die Systeme sind aber nicht so gestaltet, dass die Nutzer jede einzelne Erhebung und Verarbeitung ihrer personenbezogenen Daten in Form von inhaltlichen Beiträgen auf schwarzen Brettern, persönlichen Nachrichten oder dem Nutzungsverhalten innerhalb der Netzwerke nachvollziehen können. An wen die Daten in welcher Form weitergegeben werden oder wer sie sich einfach beschaffen kann, ist für die Nutzer kaum überschaubar. Insofern wird von einer selbstbestimmten Datenverarbeitung bei Weitem nicht in allen Fällen auszugehen sein. Daten in sozialen Netzwerken können zudem von besonderer Sensitivität sein, zumal die Nutzer mitunter zum Beispiel Angaben über ihre geschlechtliche Ausrichtung oder über ihre religiöse oder politische Überzeugung tätigen oder

diese sich aus den Aktivitäten der Nutzer erschließen lassen. Dass soziale Netzwerke inzwischen auch zur Erhebung und Verarbeitung von personenbezogenen Daten führen, die nicht einmal von Nutzern der Netzwerke stammen, zeigt das Beispiel des Facebook-*„Like-Buttons"*. Für einen Internetnutzer, der kein Mitglied von Facebook ist, der aber auf einer Webseite surft, die einen *„Like-Button"* enthält, ist überhaupt nicht erkennbar, wer hierdurch welche Daten über ihn erhebt oder verarbeitet. Von einer selbstbestimmten Verarbeitung kann hier nicht ausgegangen werden.

5.3.3 CLOUD COMPUTING

Das Cloud Computing zeichnet sich dadurch aus, dass der Nutzer Hardware, Software, Speicherplatz und Rechenkapazitäten eines Cloud-Anbieters nutzt. Dieser kann sein Angebot dadurch der Nachfrage anpassen, dass er – unter Umständen weltweit verteilte - Cloud-Ressourcen von vielen unterschiedlichen Ressourcenanbietern nutzt. Cloud Computing ist somit eine dynamische Dienstleistung, die flexibel angeboten und bedarfsorientiert abgerufen wird, die nicht von Personen, sondern durch automatische Prozesse erbracht wird und die vom Ort der Leistungserbringung unabhängig ist und daher von jedem Ort weltweit angeboten und erbracht werden kann. Cloud Computing gibt es typischerweise in verschiedenen Ausprägungen: Bei *„Infrastructure as a Service"* wird regelmäßig nur eine Infrastruktur durch den Cloud-Anbieter zur Verfügung gestellt. Bei *„Storage as a Service"* bietet der Cloud-Anbieter Speichermöglichkeiten für die personenbezogenen Daten des Cloud-Nutzers. Bei *„Software as a Service"* arbeitet der Cloud-Nutzer mit Software, die ihm der Cloud-Anbieter zur Verfügung stellt. In allen Fällen des Cloud Computing kann es sein, dass der Cloud-Nutzer personenbezogene Daten in die Cloud überträgt und diese dort vom Cloud-Anbieter auf eigenen oder fremden Ressourcen gespeichert oder verarbeitet und an den Cloud-Nutzer bei Bedarf wieder zurückübertragen werden.

Hierdurch können die Nutzer in ihrer beruflichen und unternehmerischen Freiheit nach Art. 12 Abs. 1 und Art. 14 Abs. 1 GG gefördert werden, da sie unabhängig von der Einrichtung einer eigenen IT-Infrastruktur werden und je nach Bedarf flexibel Rechenleistung und Speicherplatz „anmieten" können. Auf Anbieterseite ergeben sich Geschäftsmodelle, die ebenfalls eine Förderung der durch Art. 12 Abs. 1 und Art. 14 Abs. 1GG geschützten beruflichen und unternehmerischen Freiheit bedeuten können.

Andererseits ergeben sich durch das Cloud Computing auch spezielle Risiken. Durch eine dynamische bedarfsgesteuerte Nutzung von Cloud-Diensten kann es für die Nutzer schnell unüberschaubar werden, bei welchem Anbieter die Daten unter welchen Voraussetzungen verarbeitet werden. Wenn ein Dienst Nutzer eines Cloud-Dienstes ist und die Daten der Endnutzer an diesen weitergibt, ist für die Endnutzer meist nicht nachvollziehbar, welche Cloud-Ressourcen ihr Dienst gerade hinzubucht, um die notwendige Rechenleistung aufzubringen. Weder ist dann ohne Weiteres überschaubar, welche Daten an wen weitergegeben werden, noch, wie die Auswahl dieses Dienstes erfolgt oder aus welchem Land er unter welchem Datenschutzrecht angeboten und erbracht wird. Die informationelle Selbstbestimmung aus Art. 2 Abs. 1 und Art. 1 Abs. 1 GG wird damit durch Cloud Computing insofern infrage gestellt, dass die zur notwendigen Selbstbestimmung über die Verarbeitung personenbezogener Daten notwendigen Informationen entweder nicht vorhanden oder für den Nutzer nicht überschaubar sind. Überdies erscheint eine datenschutzrechtliche Auswahl und Kontrolle der global verteilten Cloud-Dienste durch private und gewerbliche Nutzer zunächst kaum wirkungsvoll möglich.

5.3.4 BIG DATA

Durch die immer stärkere Nutzung von Informationstechnik werden immer größere Mengen von personenbezogenen Daten verarbeitet, sowohl Daten über das Nutzungsverhalten

als auch von den Nutzern eingegebene Inhalte. Die unter dem Stichwort *„Big Data"* behandelten Datenmengen sind aus rechtlicher Sicht mit Chancen verbunden, aber auch mit erheblichen Risiken.

Gefördert werden könnte durch die große Menge an zur Verfügung stehenden Daten zum einen die Informationsfreiheit aus Art. 5 Abs. 1 GG. Auch die durch Art. 5 Abs. 3 GG geschützte Wissenschaft kann durch die Auswertung immer größerer Datenmengen zu genaueren Ergebnissen gelangen und so gefördert werden. Ebenso ergeben sich aus den neuen Möglichkeiten der Datenauswertung völlig neue Geschäftsmodelle, die durch Art. 12 Abs. 1 und Art. 14 Abs. 1 GG geschützt sein können.

Das Speichern großer Mengen personenbezogener Daten zur Verwendung über ihren ursprünglichen Zweck hinaus oder zu noch unbestimmten Zwecken widerspricht jedoch geradezu diametral dem Verbot einer anlasslosen Vorratsdatenspeicherung aus dem Volkszählungsurteil[1056] und betrifft damit das Grundrecht auf informationelle Selbstbestimmung aus Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG in seinem Kern. Gerade in Verbindung mit der im folgenden Abschnitt beschriebenen allgegenwärtigen Datenverarbeitung würde eine Speicherung großer Datenmengen auf Vorrat dazu führen, dass jederzeit detaillierte Verhaltensprofile der Nutzer erzeugt werden können. Für die Betroffenen ist kaum überschaubar, wer sich in derartigen Datenbanken bedient und welche Auswirkungen die Datenverarbeitung auf ihr Leben haben kann. Die Nutzer müssten mitunter schon davon ausgehen, dass bestimmte Akteure, wie staatliche Behörden oder große Unternehmen, entweder selbst über solche Datenbanken verfügen oder die Ressourcen haben, um potentiell alles erfahren können, was sie jemals unter Einsatz von IuK-Medien getan haben. Das Zusammentragen vieler Einzeldaten aus verschiedenen Bereichen ohne das Wissen der Betroffenen widerspricht auch unmittelbar dem Schutzgedanken des allgemeinen Persönlichkeitsrechts, dass jeder Mensch selbst darüber entscheiden darf, welche Rollen er in verschiedenen sozialen Zusammenhängen einnimmt und inwiefern er diese Rollen voneinander trennen möchte.[1057] Werden diese Datenmengen zudem zentral gespeichert, könnte ein Angreifer mit einem Schlag nicht nur einzelne, sondern weitgehende Informationen über die Betroffenen erlangen. *„Big Data"* stellt insofern ein hohes Risiko für die informationelle Selbstbestimmung dar.

5.3.5 ALLGEGENWÄRTIGE DATENVERARBEITUNG

Die Ausweitung allgegenwärtiger Datenverarbeitung bedeutet eine immer weiterreichende Durchdringung des Alltags mit Datenverarbeitung und bewirkt die Eroberung bisher datenverarbeitungsfrei funktionierender Lebensbereiche durch Datenverarbeitung.

Dies kann einerseits verfassungsrechtlich geschützte Interessen fördern. Zum Beispiel können die neuartigen Dienste den alltäglichen Handlungsrahmen der Nutzer erweitern und damit die Verwirklichungsbedingungen der allgemeinen Handlungsfreiheit aus Art. 2 Abs. 1 GG verbessern. Auch die Ausübung speziellerer Grundfreiheiten wie der Meinungs- und Informationsfreiheit aus Art. 5 Abs. 1 GG sowie der Kommunikationsfreiheit aus Art. 10 Abs. 1 kann durch die Allgegenwärtigkeit der IuK-Dienste gefördert werden. Überdies fallen die neuen Geschäftsmodelle und die damit einhergehende Datenverarbeitung in das durch Art. 12 Abs. 1 und Art. 14 Abs. 1 GG geschützte unternehmerische Interesse der Anbieter.

Andererseits führt die allgegenwärtige Datenverarbeitung zu neuen Risiken und zur Verschärfung bereits bestehender Risiken für die Grundrechte, aus denen sich die rechtliche *„Privatsphäre"* zusammensetzt. Die Allgegenwärtigkeit der Datenverarbeitung kann dazu führen, dass

1056 BVerfGE 65, 1 (46).
1057 Dreier, in: Dreier 2004, Art. 2 Abs. 1 GG, Rn. 71.

Persönlichkeitsprofile mit erheblich höherer Dichte erstellt werden können als bisher. Potentiell jede Handlung der Menschen könnte in Zukunft Datenspuren hinterlassen. Die Selbstbestimmung ist im Rahmen dieser potentiell lückenlosen Datenverarbeitung erheblich infrage gestellt. Für die Nutzer wird es immer unübersichtlicher, ob jemand, und wer wann gerade welche Daten über sie verarbeitet und wem gegenüber sie ihre Rechte auf Einsicht, Korrektur und Löschung ausüben müssten. Eine ständige selbstbestimmte Auswahl von gewollten und nicht gewollten Datenverarbeitungen im Alltag würde die Nutzer zudem völlig überfordern. Letztlich tritt das Risiko auf, dass immer weniger Lebensbereiche ohne Datenverarbeitung zu bewältigen sein werden und es somit unmöglich werden könnte, sich der Datenverarbeitung überhaupt noch zu entziehen. Diese Risiken betreffen insbesondere die informationelle Selbstbestimmung aus Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG. Aber auch das ebenfalls aus Art. 2 Abs. 1 in Verbindung mit 1 Abs. 1 GG konkretisierte Grundrecht auf Integrität und Vertraulichkeit informationstechnischer Systeme (Computergrundrecht) ist dadurch neuen Risiken ausgesetzt, dass tendenziell jedes informationstechnische System in Zukunft ständig mit anderen vernetzt sein wird und damit eine Datenerhebung von außen ermöglicht.

5.4 ÜBERBLICK ZUR DERZEITIGEN RECHTSLAGE

In diesem Abschnitt wird dargestellt, wie der Schutz der verfassungsrechtlich gewährten Privatsphäre im europäischen und deutschen Datenschutzrecht derzeit konkret ausgestaltet ist. Hierdurch wird sichtbar, wie durch den demokratisch legitimierten Gesetzgeber bisher zwischen den einander entgegenstehenden rechtlich geschützten Interessen abgewogen wurde.

5.4.1 VORGABEN DER EUROPÄISCHEN UNION

5.4.1.1 Datenschutzrichtlinie

Eine Richtlinie ist einer von fünf in Art. 288 des Vertrags über die Arbeitsweise der Europäischen Union vorgesehenen Rechtsakte der Europäischen Union. Sie ist ausschließlich an die Mitgliedstaaten gerichtet und für diese verbindlich. Für den einzelnen Bürger ist eine Richtlinie nicht unmittelbar anwendbar, bedarf also für ihre Gültigkeit innerhalb eines Staates der Umsetzung durch den nationalen Gesetzgeber. Deshalb ist eine Richtlinie streng zu unterscheiden von der Verordnung, die als Rechtsakt der Union unmittelbare Geltung für die Unionsbürger erlangt und keiner Umsetzung bedarf. Richtlinien dienen der Harmonisierung der Rechtsvorschriften in allen Mitgliedstaaten der Union, wobei der Grad der Harmonisierung entscheidend von der Ausgestaltung jeder einzelnen Richtlinie abhängt.

Die Datenschutzrichtlinie (DSRL) EG/95/46 hat zum Ziel, das Recht auf Privatsphäre natürlicher Personen sowie die weiteren Grundrechte und Grundfreiheiten bei der automatisierten und nichtautomatisierten Verarbeitung personenbezogener Daten zu schützen. Ihr Ziel ist es außerdem, einen freien Datenverkehr im Binnenmarkt auf einem einheitlichen, möglichst hohen Datenschutzniveau zu ermöglichen. In seinem Urteil vom 24.11.2011 hat der Europäische Gerichtshof – sehr zur Überraschung aller Mitgliedstaaten – festgestellt, dass die Richtlinie keine Mindest-, sondern eine Vollharmonisierung anstrebt, die Mitgliedstaaten bei der Umsetzung der Richtlinie also weder strengere noch geringere Maßstäbe ansetzen dürfen, selbst wenn sie dies wollten, um ein möglichst EU-weit einheitliches Datenschutzrecht zu verwirklichen.[1058]

Art. 6 DSRL statuiert die Grundsätze des Datenschutzes. Die personenbezogenen Daten sind demnach zweckgebunden und in rechtmäßiger Weise zu verarbeiten. Die Daten

[1058] Rechtssachen C 468/10 und C 469/10, K&R 2012, 40 – Verarbeitung personenbezogener Daten; erklärt weiterhin Art. 7 lit. f) für unmittelbar anwendbar.

müssen sachlich richtig und aktuell sein, es sind also unrichtig (gewordene) Daten zu berichtigen oder zu löschen.

Art. 7 DSRL regelt die Zulässigkeit der Verarbeitung personenbezogener Daten. Eine Verarbeitung ist danach nur möglich, wenn der Betroffene einwilligt (lit. a), wenn die Verarbeitung zur Erfüllung eines Vertrags oder einer rechtlichen Verpflichtung erforderlich ist (lit. b und c), der Wahrung lebenswichtiger Interessen der betroffenen Person dient (lit. d) oder für überwiegende öffentliche Interessen oder zur Ausübung der öffentlichen Gewalt (lit. e) oder zur Verwirklichung des berechtigten Interesses des für die Verarbeitung Verantwortlichen oder eines Dritten (lit. f) erforderlich ist. Die Regelung ist abschließend.

Art. 10 bis 12 DSRL regeln die Informationspflichten des für die Verarbeitung Verantwortlichen und das Auskunftsrecht der betroffenen Person. Es sind Informationen zu erteilen über die Identität des Verarbeitenden, die Zweckbestimmung der Verarbeitung und die Empfänger der Daten. Außerdem ist darüber zu informieren, ob die Auskunft freiwillig ist oder nicht und welche Folgen aus einer Nichtbeantwortung resultieren. Schließlich ist mitzuteilen, welche Auskunfts- und Berichtigungsrechte der betroffenen Personen zustehen. Auskunftsrechte umfassen die Fragen, ob, in welchem Umfang und zu welchem Zweck Daten erhoben und gespeichert wurden und wer von den Daten Kenntnis erlangt hat. Der Betroffene hat außerdem ein Recht auf Auskunft über die Herkunft der Daten, wenn diese von dritter Stelle erhoben wurden. Schließlich ist dem Betroffenen im Falle des Art. 7 lit. e) und f) DSRL ein Widerspruchsrecht gegen die Verarbeitung der Daten einzuräumen.

Weiterhin sind gemäß Art. 22 bis 24 DSRL von den Mitgliedstaaten Regelungen zu erlassen zu Rechtsbehelfen, Haftungsfragen und Sanktionen sowie gemäß Art. 28 eine Kontrollstelle einzurichten (Datenschutzbeauftragte). Art. 29 DSRL etabliert eine unabhängige Datenschutzgruppe, die die Kommission in Datenschutzfragen berät.[1059]

Art. 25 DSRL untersagt die Weitergabe personenbezogener Daten in Drittländer, denen es an einem vergleichbaren Datenschutzniveau mangelt. Die Feststellung darüber obliegt der Kommission und wurde bisher nur für einige wenige Länder positiv getroffen.[1060] Da dadurch der Datenaustausch zwischen Europa und den USA praktisch zum Erliegen gekommen wäre, wurde im Jahr 1998 das Datenschutzabkommen *„Safe Harbor"* geschlossen, das es europäischen Unternehmen ermöglicht, personenbezogene Daten rechtmäßig an Unternehmen in den USA zu übermitteln. Möchte ein US-amerikanisches Unternehmen dem Safe-Harbor-Abkommen beitreten, muss es sich zu den Prinzipien und FAQs des Abkommens bekennen und sich verpflichten, diese einzuhalten. Dann wird es vom US-Handelsministerium entsprechend zertifiziert. Die Europäische Kommission hat am 26. Juli 2000 entschieden, dass das Safe-Harbor-Abkommen ein angemessenes Schutzniveau im Sinne des Art. 25 Abs. 2 der Richtlinie 95/46/EG gewährleistet.[1061]

Umgesetzt wurde die Datenschutzrichtlinie in Deutschland verspätet nach einem eingeleiteten Vertragsverletzungsverfahren im Gesetz zur Änderung des Bundesdatenschutzgesetzes und anderer Gesetze vom 18. Mai 2001.[1062]

5.4.1.2 Richtlinie über den Datenschutz in der elektronischen Kommunikation

Die Richtlinie 2002/58/EG dient gemäß Art. 1 Abs. 1 der Durchsetzung des Rechts auf Privatsphäre in Bezug auf die Verarbeitung personenbezogener Daten im Bereich der elektronischen Kommunikation. Sichergestellt werden soll gemäß Art. 5 Abs. 1 die Vertraulichkeit der Kommunikation mittels öffentlicher Kommunikationsnetze und öffentlich zugänglicher Kommunikationsdienste und der damit einhergehenden Verkehrsdaten. In den Schutzbereich einbezogen

1059 Auch als Artikel-29-Datenschutzgruppe bekannt.
1060 Darunter Kanada, Schweiz und Argentinien.
1061 Entscheidung der Kommission 2000/520/EG.
1062 BGBl. I S. 904.

werden neben natürlichen erstmals auch juristische Personen. Darüber hinaus ergänzt sie die Datenschutzrichtlinie 95/46/EG und konkretisiert diese in einzelnen Bereichen.

Elektronische Kommunikation umfasst alle elektronisch übertragenen Nachrichten. Die Richtlinie regelt unter anderem den freien Verkehr der personenbezogenen Daten aus der elektronischen Kommunikation, den Umgang mit unerbetenen Nachrichten zum Zwecke der Direktwerbung mittels Telefon oder elektronischer Post sowie für Einzelgebührennachweise, Rufnummernanzeigen und Teilnehmerverzeichnisse.

Um die Vertraulichkeit der Kommunikation zu gewährleisten, ist gemäß Art. 5 der Richtlinie die Verarbeitung personenbezogener Daten nur zulässig, wenn der Nutzer sein Einverständnis nicht verweigert hat. Die Ausgestaltung der Erklärung der Einwilligung ist weit formuliert und umfasst *„jede geeignete Weise"*, zum Beispiel durch Markierung eines Feldes.[1063] Dem Betreiber obliegt es, den Nutzer umfassend über die Speicherung der Daten sowie über Zwecke der Verarbeitung aufzuklären und auf sein Recht zur (auch nachträglichen) Verweigerung seines Einverständnisses hinzuweisen.

Verkehrsdaten sind solche zur Übertragung einer Nachricht an ein elektronisches Kommunikationsnetz. Diese sind umgehend zu löschen oder zu anonymisieren, sobald sie nicht mehr zur Übertragung einer Nachricht benötigt werden oder der Teilnehmer für Dienste mit Zusatznutzen in die Verarbeitung eingewilligt hat.

Dienste mit Zusatznutzen umfassen insbesondere solche für *Location Based Services* auf mobilen Endgeräten wie Smartphones, die der Verkehrsnavigation dienen oder zur Suche jeglicher denkbarer Informationen genutzt werden können (Points of Interest, Hotels, U-Bahn-Haltestellen, Restaurants). Hierfür wird die Verarbeitung von Standortdaten, also aller Daten, die bei der elektronischen Kommunikation verarbeitet werden und die geographische Standortbestimmung des Nutzers ermöglichen, für zulässig erachtet, wenn der Nutzer eingewilligt hat. Die Einwilligung ist jederzeit widerruflich. Die Verarbeitung der Daten ist streng zweckgebunden. Es ist der Grundsatz der Datensparsamkeit zu beachten, es sind also nur erforderliche Daten zu erheben und nur so lange wie unbedingt nötig zu speichern.

Die Verarbeitung personenbezogener Daten zum Zwecke der Direktwerbung mittels unerbetener Nachrichten wird erstmals gesetzlich geregelt. Es soll darauf jedoch an dieser Stelle nicht näher eingegangen werden, da durch die Cookie-Richtlinie (siehe sogleich) umfangreiche Änderungen vorgenommen worden sind.

Die Richtlinie wurde durch die Bundesrepublik – wiederum verspätet – in nationales Recht umgesetzt. Hierzu wurde das Telekommunikationsgesetz einer grundlegenden Neufassung unterzogen und trat in dieser Form 2004 in Kraft.

5.4.1.3 Cookie-Richtlinie

Die Richtlinie 2009/136/EG (Cookie-Richtlinie) konkretisiert und modernisiert die Richtlinie zur elektronischen Kommunikation (2002/58/EG) in vielerlei Hinsicht. Sie dient dem verbesserten Schutz der Privatsphäre und Vertraulichkeit sowie personenbezogener Daten des Einzelnen, auch um wirtschaftliche Schäden bis hin zu Identitätsbetrug und soziale Nachteile zu vermeiden.[1064] Gleichzeitig fordert die Richtlinie den weiteren Ausbau der öffentlichen Kommunikationssysteme und der Anschlüsse der Nutzer.

Die Cookie-Richtlinie betrifft neben Cookies alle Arten von Software, die es dem Anwender ermöglichen, nutzerbezogene Daten zu erheben, zu speichern und zu verarbeiten, wie Spähsoftware oder Viren.[1065]

1063 Erwägungsgrund 17.
1064 Erwägungsgrund 26 und 61.
1065 Erwägungsgrund 65 und 66.

Der Zugriff auf im Endgerät des Nutzers gespeicherte Informationen und deren Speicherung ist nur nach vorheriger Einwilligung des Nutzers gestattet. Der Begriff der speicherbaren Information ist nicht näher definiert und wird wohl im Sinne der Richtlinie weit auszulegen sein. Eine Ausnahme sieht die Richtlinie für solche Cookies vor, die notwendig sind, um den Dienst zu erbringen oder die Teilnahme zu ermöglichen (sogenannte Session-Cookies).[1066] Die Einwilligung hat auf Grundlage umfassender, klarer und verständlicher Information über den Zweck der Verarbeitung und das Recht auf Widerspruch zu erfolgen.[1067] Die Einwilligung kann im Einklang mit der Datenschutzrichtlinie 95/46/EG über entsprechende Browsereinstellungen erteilt werden, wenn dies technisch durchführbar und wirksam ist.[1068]

Das Verbot unerbetener Nachrichten zu Zwecken der Direktwerbung wird auf alle elektronischen Kommunikationssysteme (E-Mail, SMS/MMS) ausgeweitet, sofern nicht der Nutzer seine vorherige ausdrückliche Einwilligung erteilt hat. Neben dem generellen Verbot der anonymen Direktwerbung, die bereits in der Datenschutzrichtlinie zur elektronischen Kommunikation eingeführt wurde, ist es dem Betreiber nun zusätzlich untersagt, den Nutzer aufzufordern, Webseiten aufzurufen (per Hyperlink), die gegen dieses Verbot verstoßen.

Die Sicherheit der Verarbeitung wird neu definiert. So ist sicherzustellen, dass nur ermächtigte Personen für rechtlich zulässige Zwecke Zugang zu personenbezogenen Daten erhalten, gespeicherte Daten vor Zerstörung, Verarbeitung und Weitergabe besonders zu schützen sind und ein Sicherheitskonzept für die Verarbeitung ein- und effektiv umgesetzt wird.[1069] Weiterhin werden detailliert die Pflichten der Betreiber geregelt, wenn Verletzungen des Schutzes personenbezogener Daten festgestellt werden.[1070] So sind der zuständige Datenschutzbeauftragte sowie der betroffene Nutzer zu informieren und geeignete Abhilfemaßnahmen zu ergreifen.

Die Richtlinie war von den Mitgliedstaaten bis Mai 2011 umzusetzen. Der deutsche Gesetzgeber ist dem bislang nicht nachgekommen. Der derzeitige Gesetzesentwurf zur Umsetzung befindet sich im Bundestag und sieht eine Neufassung des § 13 TMG vor. Ein neuer Abs. 8 soll im Wesentlichen den Wortlaut des Art. 2 Nr. 5 der Richtlinie wiedergeben. Außerdem soll ein neuer § 13a TMG eingeführt werden, der umfangreiche Informations- und Organisationspflichten für Diensteanbieter vorschreibt.[1071]

5.4.2 GRUNDZÜGE DES DEUTSCHEN DATENSCHUTZRECHTS

5.4.2.1 Systematik

Das Recht auf informationelle Selbstbestimmung wird nicht schrankenlos gewährt. Der Staat benötigt zur Erfüllung seiner Aufgaben Daten seiner Bürger und auch die private Wirtschaft ist auf die Verarbeitung personenbezogener Daten angewiesen, zum Beispiel um Verträge abwickeln zu können. Die im Folgenden erläuterten Datenschutzgesetze sind daher Ermächtigungen und Erlaubnisse zum Umgang mit personenbezogenen Daten innerhalb bestimmter Grenzen, unter bestimmten Voraussetzungen auch ohne oder sogar gegen den Willen des Betroffenen. Konkretisiert wird das informationelle Selbstbestimmungsrecht einfachgesetzlich zunächst durch die allgemeinen Datenschutzgesetze des Bundes (BDSG) und der Länder (LDSG),[1072] die als Auffanggesetze[1073] fungieren. Hinzu

1066 Art. 2 Nr. 5 Satz 2 der Richtlinie.
1067 Art. 2 Nr. 5 der Richtlinie 2009/136/EG.
1068 Erwägungsgrund 66.
1069 Art. 2 Nr. 4 a) und b) der Richtlinie.
1070 Art. 2 Nr. 4 c) der Richtlinie.
1071 BR-Drucks. 156/11 und BT-Drucks. 17/6765.
1072 Das bereits 1970 erlassene Hessische Datenschutzgesetz gilt als das erste Datenschutzgesetz der Welt.
1073 Gola / Schomerus 2010, § 1 BDSG, Rn. 24.

kommen bereichsspezifische Sonderreglungen. Während das Bundesdatenschutzgesetz den Umgang mit personenbezogenen Daten durch die Bundesbehörden und die Privatwirtschaft regelt, ist Inhalt der Landesdatenschutzgesetze der Umgang mit personenbezogenen Daten durch die Landesbehörden. Die bereichsspezifischen Spezialregelungen gehen diesen allgemeinen Gesetzen vor, jene kommen nur zur Anwendung, soweit keine Spezialnorm existiert. Der Umgang mit personenbezogenen Daten durch die Behörden der Sozialversicherungen ist zum Beispiel im Sozialgesetzbuch (SGB) geregelt, der der Polizeibehörden in den jeweiligen Polizeigesetzen, der der Anbieter von Telemediendiensten (zum Beispiel soziale Netzwerke und Suchmaschinen) im Telemediengesetz (TMG).

5.4.2.2 Datenschutzprinzipien

Aus dem Recht auf informationelle Selbstbestimmung ergeben sich einige Grundprinzipien des Datenschutzrechts, die sich in den verschiedenen Gesetzen wiederfinden:

Notwendigkeit einer Erlaubnis

Die automatisierte Verarbeitung personenbezogener Daten eines Betroffenen stellt einen Eingriff in dessen informationelles Selbstbestimmungsrecht dar. Ein solcher Grundrechtseingriff bedarf, um rechtmäßig zu sein, einer Rechtfertigung. Dies bedeutet, dass die automatisierte Datenverarbeitung nur soweit zulässig ist, wie eine Rechtsvorschrift sie erlaubt oder der Betroffene eingewilligt hat.[1074] Jede Phase des Umgangs mit personenbezogenen Daten (Erhebung, Speicherung, weitere Nutzung) ist dabei gesondert zu betrachten und muss jeweils einzeln geprüft werden. Gemäß der abschließenden Aufzählung in § 4 Abs. 1 BDSG ist die Verwendung personenbezogener Daten daher nur insoweit zulässig wie:

- das BDSG sie erlaubt,
- eine andere Rechtsvorschrift sie erlaubt oder
- der Betroffene eingewilligt hat.[1075]

Direkterhebungsgrundsatz

Auch wenn eine Erlaubnisnorm vorliegt, muss die Datenerhebung gemäß § 4 Abs. 2 BDSG grundsätzlich direkt beim Betroffenen erfolgen, damit dieser von der Datenerhebung Kenntnis hat.[1076] Datenerhebungen ohne Mitwirkung und Kenntnis des Betroffenen sind nur in gesetzlich geregelten Ausnahmefällen zulässig. Keine Umgehung des Direkterhebungsgrundsatzes liegt allerdings dann vor, wenn die Daten *auch* eine weitere Person betreffen.[1077]

Zweckbindungsgrundsatz

Personenbezogene Daten dürfen grundsätzlich nur zu jeweils vorher bestimmten Zwecken erhoben, verarbeitet und genutzt werden, die für den Betroffenen erkennbar sein müssen.[1078] Der zulässige Zweck einer Datenerhebung, -verarbeitung oder -nutzung ergibt sich aus der jeweiligen Erlaubnisnorm. Zweckänderungen, also die Verarbeitung oder Nutzung personenbezogener Daten zu anderen als den ursprünglichen Zwecken, bedürfen einer besonderen Erlaubnis, zum Beispiel §§ 14 Abs. 2 und 28 Abs. 2 BDSG. Eine besonders strenge Zweckbindung besteht nach § 39 BDSG für Daten, die einem Berufs- oder Amtsgeheimnis unterliegen. Personenbezogene Daten, die ausschließlich der Datenschutzkontrolle oder der Datensicherung dienen, dürfen gar nicht zweckfremd verwendet werden, siehe §§ 14 Abs. 4 und 31 BDSG. Die Zweckbindung ist insbesondere auch durch technische Maßnahmen sicherzustellen.[1079] So verlangt Ziffer 8 der Anlage zu § 9 BDSG, zu unterschiedlichen Zwecken erhobene Daten getrennt zu verarbeiten.

1074 Sokol, in: Simitis 2011, § 4 BDSG, Rn. 2.
1075 Moos 2006, 45.
1076 Sokol, in: Simitis 2011, § 4 BDSG, Rn. 23.
1077 Gola / Schomerus 2010, § 4 BDSG, Rn. 20.
1078 BVerfGE 65, 1 (46); Moos, Datenschutzrecht - Schnell erfasst, 2006, 50.
1079 Schultze-Melling, in: Taeger / Gabel 2010, § 9 BDSG, Rn. 79.

Erforderlichkeit

Der Grundsatz der Erforderlichkeit steht in engem Zusammenhang mit der Zweckbindung. Er beschränkt den Umgang mit personenbezogenen Daten auf das für die Erreichung des jeweiligen Zwecks erforderliche Maß. Dies bedeutet, dass der verfolgte legitime Zweck nicht mit einem geringeren Maß an Datenerhebung, -verarbeitung oder -nutzung genauso gut verwirklicht werden könnte. Erforderlichkeit der Erhebung, Verarbeitung oder Nutzung personenbezogener Daten besteht also dann, wenn keine ebenso effektive Alternative mit geringerer Eingriffstiefe vorhanden ist. Der Grundsatz der Erforderlichkeit kommt zum Beispiel in §§ 13 Abs. 1 und 28 Abs. 1 Nr. 1 und 2 BDSG zum Ausdruck.

Grundsatz der Datenvermeidung und Datensparsamkeit

In § 3a BDSG kommt der Grundsatz der Datenvermeidung und Datensparsamkeit zum Ausdruck. Er ist mit dem Erforderlichkeitsgrundsatz nicht identisch. Der Grundsatz der Erforderlichkeit überlässt die Wahl des Zwecks der Datenverarbeitung der verantwortlichen Stelle und fragt nur, ob der Umfang der Datenerhebung, -verarbeitung und -nutzung erforderlich ist, diesen Zweck zu erreichen. Dagegen bezieht sich der Grundsatz der Datenvermeidung und Datensparsamkeit auf diesen Zweck und fragt, ob der Zweck so gewählt werden kann (zum Beispiel Flatrate statt nutzungsspezifischer Abrechnung), dass durch die Gestaltung und Auswahl von Datenverarbeitungsanlagen die Verarbeitung personenbezogener Daten vermieden und vermindert werden kann. Datenverarbeitende Stellen sollen durch den Einsatz datenvermeidender Anlagen auf technischem Weg den Datenschutz von vornherein verwirklichen.[1080]

Transparenz

Das Transparenzgebot soll dafür sorgen, dass die Betroffenen davon Kenntnis haben, welche ihrer Daten in welchem Umfang erhoben, verarbeitet oder genutzt werden.[1081] Schon der Direkt-erhebungsgrundsatz soll dafür sorgen, dass ein Betroffener von einer Datenerhebung erfährt und selbst entscheiden kann, ob er die Daten herausgeben will oder nicht. Gemäß § 4 Abs. 3 BDSG ist der Betroffene bei der Direkterhebung daher umfassend zu informieren. In den Fällen, in denen der Direkterhebungsgrundsatz nicht gilt, ist der Betroffene im Nachhinein über den ihn betreffenden Umgang mit personenbezogenen Daten nach § 33 BDSG zu benachrichtigen. Auch muss auf Antrag den Betroffenen Auskunft über sie betreffende Datenerhebung, -verarbeitung und -nutzung gegeben werden, zum Beispiel gemäß §§ 19 und 34 BDSG. Datenverarbeitende Stellen haben gemäß §§ 4g Abs. 2 in Verbindung mit 4e BDSG für jedes automatisierte Datenverarbeitungsverfahren ein Verfahrensverzeichnis anzulegen, das dem betrieblichen Datenschutzbeauftragten zur Veröffentlichung zu übergeben ist.

Korrektur- und Abwehrrechte

Zur Verwirklichung der informationellen Selbstbestimmung und um den Risiken unrichtiger oder unzulässiger Datenerhebung, -verarbeitung und -nutzung entgegenzuwirken, sind den Betroffenen Rechte auf Korrektur und Löschung der über sie gespeicherten Daten einzuräumen.[1082] Solche finden sich zum Beispiel in den §§ 20 und 35 BDSG. Daneben sind, zum Beispiel in den §§ 7 und 8 BDSG, Schadensersatzansprüche bei unzulässigem Datenumgang etabliert. Die Schadensersatzansprüche gegen private Stellen sind dabei als Verschuldenshaftung, die gegen öffentliche Stellen als Gefährdungshaftung ausgestaltet. Dies bedeutet, dass die Betroffenen gegenüber den öffentlichen Stellen lediglich den unzulässigen Datenumgang nachweisen müssen, um mit dem Anspruch im Prozess erfolgreich zu sein. Private Stellen hingegen können sich gemäß § 7 Satz 2 BDSG bezüglich ihres Verschuldens exkulpieren.[1083]

1080 Roßnagel 2011.
1081 Sokol, in: Simitis 2011, § 4 BDSG, Rn. 39.
1082 Siehe zum Beispiel BVerfGE 65, 1 (46).
1083 Roßnagel / Pfitzmann / Garstka 2001, S. 179 ff.

5.4.2.3 Bundesdatenschutzgesetz

Die Grundzüge des deutschen Datenschutzrechts werden im Folgenden anhand des Bundesdatenschutzgesetzes dargestellt, dem die Landesdatenschutzgesetze, die für die öffentlichen Stellen der Länder gelten, insoweit weitgehend entsprechen.

Wichtige Grundbegriffe

Das Bundesdatenschutzgesetz definiert einige zentrale Begriffe des Datenschutzrechts, die sich in den verschiedensten Erlaubnisnormen wiederfinden und bestimmte Rechtsfolgen auslösen können:

> Personenbezogene Daten

Personenbezogene Daten sind gemäß § 3 Abs. 1 BDSG alle Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person. Diese Person wird im Bundesdatenschutzgesetz als Betroffener bezeichnet. Personenbezogen sind Daten, wenn sie Angaben enthalten, die direkt auf die Person des Betroffenen schließen lassen. Personenbeziehbarkeit ist gegeben, wenn die betroffene Person durch eigenes oder – in verhältnismäßiger Weise – mobilisierbares Zusatzwissen identifiziert werden kann. Da dieses Zusatzwissen unter Beachtung vorhandener Ressourcen für jede verantwortliche Stelle unterschiedlich ist, muss der Personenbezug relativ zu den Möglichkeiten der jeweiligen verantwortlichen Stelle bestimmt werden.[1084] In § 3 Abs. 9 BDSG sind besondere Arten personenbezogener Daten genannt, deren Erhebung, Verarbeitung und Nutzung besonders strengen Voraussetzungen unterliegt: Angaben über die rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit oder Sexualleben.

> Schritte des Umgangs mit personenbezogenen Daten

§ 3 Abs. 2 BDSG definiert das Erheben als das Beschaffen von personenbezogenen Daten. In § 3 Abs. 3 BDSG wird das Verarbeiten als das Speichern, Verändern, Übermitteln, Sperren und Löschen bestimmt. In § 3 Abs. 4 BDSG ist noch das Nutzen als jedwede Verwendung personenbezogener Daten definiert, die keine Verarbeitung im Sinne des vorigen Absatzes darstellt. Diese Begriffe sind dazu bestimmt, alle Schritte eines Umgangs mit personenbezogenen Daten abzudecken[1085] und bilden den Anknüpfungspunkt für die Voraussetzungen der Erlaubnisnormen. Eine rein persönliche oder familiäre Erhebung, Verarbeitung oder Nutzung durch Private fällt gemäß § 1 Abs. 2 Nr. 3 BDSG nicht in den Anwendungsbereich des Gesetzes und ist allgemein zulässig.[1086]

> Automatisierte Verarbeitung

Automatisierte Verarbeitung ist gemäß § 3 Abs. 2 die Erhebung, Verarbeitung oder Nutzung personenbezogener Daten unter Einsatz von Datenverarbeitungsanlagen. Der Anwendungsbereich des Gesetzes erstreckt sich gemäß § 1 Abs. 2 Nr. 1 und Nr. 2 BDSG für den öffentlichen Bereich zwar auf jede Art der Datenverarbeitung. Gemäß Nr. 3 ist das Bundesdatenschutzgesetz für private Stellen aber nur insoweit anwendbar, wie sie Datenverarbeitungsanlagen oder nicht automatisierte Dateien verwenden. Gerade im privaten Sektor kommt dem Begriff der automatisierten Verarbeitung damit eine besondere Bedeutung zu. Für den Bereich des Beschäftigtendatenschutzes ist allerdings zu beachten, dass hier nicht lediglich die automatisierte Datenverarbeitung, sondern jeder Umgang mit personenbezogenen Daten, den Regelungen über den Datenschutz im Beschäftigungsverhältnis unterfällt. Dies gilt sowohl nach bereits bestehender Rechtslage gemäß § 32 Abs. 2 BDSG, wie auch nach dem Gesetzentwurf zur Neuregelung des Beschäftigtendatenschutzes, dann gemäß § 27 Abs. 3 BDSG n. F.[1087]

> Verantwortliche Stelle

Als verantwortliche Stelle wird gemäß § 3 Abs. 7 BDSG jede Person oder Stelle bezeichnet, die personenbezogene

1084 Bergmann / Möhrle / Herb 2011, § 3 BDSG, Rn. 16.
1085 Dammann, in: Simitis 2011, § 3 BDSG, Rn. 111.
1086 Gola / Schomerus 2010, § 1 BDSG, Rn. 21.
1087 BT-Drs.17/4230.

Daten für sich selbst erhebt, verarbeitet oder nutzt oder dies durch andere im Auftrag vornehmen lässt.[1088] Die verantwortliche Stelle ist der Adressat der datenschutzrechtlichen Erlaubnisnormen und unterliegt der Kontrolle durch die Aufsichtsbehörden.

> Anonymisieren und Pseudonymisieren

Anonymisieren ist gemäß § 3 Abs. 6 BDSG das Verändern personenbezogener Daten derart, dass der Personenbezug nicht mehr oder nur mit unverhältnismäßig hohem Aufwand hergestellt werden kann. Jeglicher Bezug zum Betroffenen wird hierbei gelöscht oder von vornherein vermieden. Anonymisierte Daten stellen keine personenbezogenen Daten im Sinne des Bundesdatenschutzgesetzes dar und unterliegen daher nicht den Anforderungen der Datenschutzregelungen.[1089]

Im Gegensatz dazu wird bei einer Pseudonymisierung gemäß § 3 Abs. 6a BDSG die Zuordnung der Daten zu dem Betroffenen nur erschwert. Der Name des Betroffenen und andere Identifizierungsmerkmale werden durch ein Pseudonym ersetzt, das jedoch anhand einer Referenz noch zugeordnet werden kann. Pseudonymisierte Daten gelten gegenüber dem Referenzinhaber weiterhin als personenbezogene Daten.[1090]

Gemeinsame Vorschriften für den öffentlichen und nicht öffentlichen Bereich

Das Bundesdatenschutzgesetz enthält im ersten Abschnitt Vorschriften, die für öffentliche und private Stellen gleichsam gelten. Neben der in § 4a BDSG geregelten Einwilligung sind hier insbesondere die automatisierte Einzelentscheidung, die Meldepflicht, die Auftragsdatenverarbeitung, die Vorschriften über die internen Datenschutzbeauftragten und über technische und organisatorische Datenschutzmaßnahmen zu nennen.

> Einwilligung

Eine Einwilligung liegt gemäß § 4a Abs. 1 Satz 1 BDSG nur dann vor, wenn es sich um eine freiwillige Entscheidung des Betroffenen handelt, wobei dieser gemäß Satz 2 über den beabsichtigten Umgang mit den ihn betreffenden Daten umfassend zu informieren ist.[1091] Die Einwilligung muss ohne Zwang erfolgen. Dies kann dann nicht gegeben sein, wenn dem Betroffenen bei Verweigerung der Einwilligung Nachteile durch die verantwortliche Stelle drohen.[1092] Die Einwilligung muss gemäß § 4a Abs. 1 Satz 3 BDSG grundsätzlich in Schriftform erfolgen, kann aber unter besonderen Umständen auch in anderer Form abgegeben werden.

> Automatisierte Einzelentscheidung

Gemäß § 6a Abs. 1 BDSG dürfen Entscheidungen, die für den Betroffenen eine rechtliche Folge nach sich ziehen, nicht lediglich aufgrund einer automatisierten Verarbeitung personenbezogener Daten erfolgen, die der Bewertung einzelner Persönlichkeitsmerkmale dient. Die Vorschrift verfolgt den Zweck, dass wenigstens ein Mensch an solchen Entscheidungen mitwirkt und der Betroffene eine Gelegenheit erhält, seinen Standpunkt zu erklären.[1093] Im öffentlichen Bereich sind hier in erster Linie Verwaltungsakte zu nennen.[1094] Rein tatsächliche Abläufe, die nur Ausführungen zugrunde liegender Verträge darstellen, fallen nicht unter die Vorschrift, wie etwa das Abheben von Geld am Automaten.[1095] Auch bloße Vorentscheidungen, wie etwa eine nach bestimmten Merkmalen automatisierte Vorauswahl im

1088 Buchner, in: Taeger / Gabel 2010, § 3 BDSG, Rn. 52 ff.
1089 Gola / Schomerus 2010, § 3 BDSG, Rn. 43.
1090 Scholz, in: Simitis 2011, § 3 BDSG, Rn. 217.
1091 Bergmann / Möhrle / Herb 2011, § 4a BDSG, Rn. 5 und 11.
1092 Simitis, in: Simitis 2011, § 4a BDSG, Rn. 62 ff.
1093 Gola / Schomerus 2010, § 6a BDSG, Rn. 1 und 3.
1094 Mackenthun, in: Taeger / Gabel 2010, § 6a BDSG, Rn. 11.
1095 Gola / Schomerus 2010, § 6a BDSG, Rn. 4.

Rahmen einer Stellenbesetzung im Abgleich mit bestimmten Merkmalen des Personalbestands sind nicht von § 6b Abs. 1 BDSG umfasst.[1096]

> Meldepflicht

Gemäß § 4d Abs. 1 BDSG sind öffentliche und private Stellen verpflichtet, Verfahren automatisierter Datenverarbeitungen vor deren Inbetriebnahme der zuständigen Aufsichtsbehörde zu melden. Durch die Ausnahmevorschriften der Abs. 2 und 3 wird diese Pflicht aber selbst zum Ausnahmefall.[1097] Gemäß Abs. 2 entfällt die Pflicht durch Bestellung eines betrieblichen oder behördlichen Datenschutzbeauftragten. Sie entfällt gemäß Abs. 3 auch, wenn die verantwortliche Stelle Daten für eigene Zwecke erhebt, verarbeitet und nutzt, hiermit in der Regel höchstens neun Mitarbeiter beschäftigt sind und als Grundlage der Datenverarbeitung entweder eine Einwilligung des Betroffenen dient oder die Erhebung, Verarbeitung oder Nutzung im Rahmen der Bearbeitung eines Vertragsverhältnisses oder vertragsähnlichen Schuldverhältnisses mit dem Betroffenen erforderlich ist. Bei solchen Datenverarbeitungsanlagen gelten Beeinträchtigungen der Freiheitsrechte der Betroffenen als relativ unwahrscheinlich, die Vorschrift soll daher kleinere Unternehmen entlasten.[1098] Beispiele wären Datenverarbeitungen durch Selbständige wie Ärzte oder Apotheker und durch Kleingewerbetreibende. Eine Rückausnahme gemäß Abs. 4 gilt allerdings für Stellen, deren Geschäft gerade im Umgang mit personenbezogenen Daten besteht, wie etwa Auskunfteien, Adresshändler oder Marktforschungsunternehmen. Der Inhalt der Meldepflicht ergibt sich aus § 4e BDSG. Die gemeldeten Informationen werden mit Ausnahme der Beschreibung nach § 4e Satz 1 Nr. 9 BDSG gemäß § 38 Abs. 2 BDSG von der Aufsichtsbehörde als Register veröffentlicht.

> Auftragsdatenverarbeitung

Eine Auftragsdatenverarbeitung nach § 11 BDSG liegt dann vor, wenn eine Stelle eine andere Stelle oder Person mit der Erhebung, Verarbeitung oder Nutzung personenbezogener Daten beauftragt. Der Auftraggeber bleibt in diesem Fall verantwortliche Stelle im Sinne des § 3 Abs. 7 BDSG. Der Auftragnehmer ist von ihm gemäß § 11 Abs. 2 Satz 1 BDSG sorgfältig insbesondere unter Berücksichtigung der Eignung der von ihm getroffenen technischen und organisatorischen Maßnahmen auszuwählen. Der Auftrag ist gemäß § 11 Abs. 2 Satz 2 BDSG schriftlich zu erteilen und muss die Einzelheiten des Auftragsverhältnisses im Hinblick auf den Datenschutz gemäß der Nr. 1 bis 10 festlegen.

Die Auftragsdatenverarbeitung ist von der Funktionsübertragung abzugrenzen, bei der die andere Stelle nicht mehr bloß eine Hilfsfunktion für die verantwortliche Stelle übernimmt. Vielmehr wird die zugrunde liegende Aufgaben übertragen oder sie verfolgt mittels der übertragenen Daten eigene Geschäftszwecke. In einem solchen Fall wird die Stelle, an welche die Daten weitergegebenen werden, selbst zur verantwortlichen Stelle und die Weitergabe der Daten ist als Übermittlung im Sinne des § 3 Abs. 4 BDSG zu klassifizieren.[1099]

> Behördliche und betriebliche Datenschutzbeauftragte

Öffentliche und private Stellen, die personenbezogene Daten automatisiert verarbeiten, haben gemäß § 4f Abs. 1 Satz 1 BDSG einen behördlichen beziehungsweise betrieblichen Datenschutzbeauftragten zu bestellen. Nicht zur Bestellung eines eigenen Datenschutzbeauftragten verpflichtet sind gemäß Satz 3 private Stellen, bei denen in der Regel höchstens neun Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt sind. Zum Beauftragten für Datenschutz können gemäß § 4f Abs. 2 BDSG nur solche Personen ernannt werden, die die notwendige Fachkunde besitzen. Das Maß an Fachkunde bestimmt sich insbesondere nach dem Umfang der Datenverarbeitung und dem Schutzbedarf des Betroffenen im Hinblick auf die konkreten Daten. Diese Fachkunde kann zum Beispiel in Weiterbildungen zum

1096 Scholz, in: Simitis 2011, § 6a BDSG, Rn. 16.
1097 Gola / Schomerus 2010, § 4d BDSG, Rn. 6.
1098 Scheja, in: Taeger / Gabel 2010, § 4d BDSG, Rn. 23 f.
1099 Petri, in: Simitis 2011, § 11 BDSG, Rn. 22.

Datenschutz erworben werden.[1100] Zulässig ist auch, die Aufgabe des internen Datenschutzbeauftragten an externe Stellen zu vergeben, die in diesem Gebiet spezialisiert sind. Aufgabe des Datenschutzbeauftragten ist es gemäß § 4g BDSG, in seiner Behörde oder in seinem Betrieb auf die Einhaltung der Datenschutzregelungen hinzuwirken. Zu diesem Zweck kann er sich jederzeit an die Aufsichtsbehörden wenden und deren Beratung in Anspruch nehmen. Er ist dem Leiter der Stelle unmittelbar zu unterstellen und auf dem Gebiet des Datenschutzes weisungsfrei.[1101] Die jeweilige Stelle hat ihren Datenschutzbeauftragten bei seiner Arbeit zu unterstützen, ihm insbesondere Räume, Hilfspersonal und Hilfsmittel zur Verfügung zu stellen, soweit dies zur Aufgabenerfüllung notwendig ist. Betroffene können sich jederzeit an den Datenschutzbeauftragten wenden.

> Technische und organisatorische Maßnahmen

Die verantwortlichen Stellen haben gemäß § 9 BDSG technische und organisatorische Maßnahmen zu treffen, die erforderlich sind, um die Ziele des Gesetzes, insbesondere die in der Anlage zu § 9 BDSG konkretisierten Ziele zu verwirklichen und einem Missbrauch von personenbezogenen Daten oder Fehlern im Umgang mit diesen vorzubeugen. Erforderlich sind solche Maßnahmen allerdings nur, soweit sie zum Schutzzweck in einem angemessenen Verhältnis stehen.[1102] Die Ziele der zu ergreifenden Maßnahmen sind in der Anlage zu § 9 BDSG beschrieben: Zutrittskontrolle, Zugangskontrolle, Zugriffskontrolle, Weitergabekontrolle, Eingabekontrolle, Auftragskontrolle, Verfügbarkeitskontrolle und Trennung von Daten, die zu unterschiedlichen Zwecken erhoben wurden.

Erlaubnistatbestände für öffentliche Stellen

Die allgemeinen Rechtsgrundlagen der Datenverarbeitung durch die öffentlichen Stellen des Bundes finden sich in den §§ 12 bis 18 BDSG.

Gemäß § 13 Abs. 1 BDSG ist das Erheben personenbezogener Daten nur soweit zulässig, wie dies zur Erfüllung der Aufgaben der verantwortlichen Stelle erforderlich ist. Diese zunächst sehr weit scheinende Erlaubnis ist unter den bereits dargestellten Prinzipien der Zweckbindung und Erforderlichkeit zu sehen, die in § 13 Abs. 1 BDSG erkennbar sind.[1103] Die öffentliche Stelle ist von vornherein auf die Zwecke beschränkt, die sie im Rahmen der ihr zugewiesenen Aufgaben zu erfüllen hat. Nur eine Datenverarbeitung, die zum Erreichen dieser Zwecke erforderlich ist, ist zulässig. Das Erheben der besonderen Arten personenbezogener Daten im Sinne des § 3 Abs. 9 BDSG ist nur nach den strengeren Voraussetzungen des § 13 Abs. 2 BDSG zulässig. Das Speichern, Verändern oder Nutzen personenbezogener Daten ist gemäß § 14 Abs. 1 Satz 1 BDSG zulässig, soweit es zur Erfüllung der Aufgaben der verantwortlichen Stelle erforderlich ist und für die Zwecke erfolgt, für die die Daten erhoben worden sind. Das Speichern, Verändern oder Nutzen zu anderen Zwecken (Zweckänderung) ist nur unter den Voraussetzungen des § 14 Abs. 2 BDSG zulässig. In den §§ 15 und 16 BDSG ist die Übermittlung personenbezogener Daten an andere öffentliche Stellen und an private Stellen geregelt.

Erlaubnistatbestände für private Stellen

Die wichtigsten Erlaubnisnormen des Bundesdatenschutzgesetzes für die Erhebung, Verarbeitung und Nutzung personenbezogener Daten durch private Stellen finden sich in § 28 BDSG.

§ 28 Abs. 1 Satz 1 Nr. 1 bis 3 BDSG erlaubt das Erheben, Speichern, Verändern und Übermitteln personenbezogener Daten oder ihre Nutzung als Mittel für die Erfüllung eigener Geschäftszwecke in drei Fällen:

1100 Siehe zum Beispiel Gola / Schomerus 2010, § 4f BDSG, Rn. 20 f.
1101 Siehe zum Beispiel Scheja, in: Taeger / Gabel 2010, § 4d BDSG, Rn. 81 f.
1102 Siehe zum Beispiel Ernestus, in: Simitis 2011, § 9 BDSG, Rn. 38.
1103 Bergmann / Möhrle / Herb 2011, § 13 BDSG, Rn. 22 ff; Gola/Schomerus 2010, § 13 BDSG, Rn. 3.

- wenn es für die Begründung, Durchführung oder Beendigung eines rechtsgeschäftlichen oder rechtsgeschäftsähnlichen Schuldverhältnisses mit dem Betroffenen erforderlich ist (Nr.1),
- soweit es zur Wahrung berechtigter Interessen der verantwortlichen Stelle erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Verarbeitung oder Nutzung überwiegt (Nr. 2),
- wenn die Daten allgemein zugänglich sind und das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Verarbeitung oder Nutzung gegenüber dem berechtigten Interesse der verantwortlichen Stelle nicht offensichtlich überwiegt (Nr. 3).

Nr. 1 spielt für die Privatwirtschaft eine wichtige Rolle, da eine solche Datenverarbeitung für die Durchführung von Verträgen essentiell ist. Wann eine Datenverarbeitung im Sinne der Nr. 1 vorliegt, ist nach dem jeweiligen Zweck des Schuldverhältnisses zu bestimmen.[1104] Hierzu zählen in erster Linie solche Datenverarbeitungen, die für die Erfüllung der vertraglichen Pflichten erforderlich sind (zum Beispiel Kontodaten für die Zahlung, Anschrift für die Lieferung).

Ein berechtigtes Interesse der verantwortlichen Stelle im Sinne der Nr. 2 ist ein nach vernünftiger Erwägung der Sachlage gerechtfertigtes Interesse. Dieses kann rein wirtschaftlicher oder sogar ideeller Natur sein, solange es zur Erfüllung von Geschäftszwecken der verantwortlichen Stelle im weitesten Sinne erforderlich ist.[1105] Die notwendige Interessenabwägung kann insbesondere dann zugunsten des Betroffenen ausschlagen und die Datenverarbeitung unzulässig werden, wenn es sich um Daten aus der Intimsphäre handelt, um Daten im Sinne des § 3 Abs. 9 BDSG oder wenn die Daten dazu verwendet werden, Persönlichkeitsprofile der Betroffenen zu erstellen.

Als allgemein zugängliche Quelle im Sinne des § 28 Abs. 1 Satz 1 Nr. 3 ist neben Zeitungen, Zeitschriften und Rundfunk grundsätzlich auch das Internet anzusehen, soweit die Daten nicht besonders gegen Zugriff gesichert sind. Daten in sozialen Netzwerken, die nicht auf bestimmte Nutzergruppen beschränkt sind, zählen dazu.[1106] Ein offensichtliches Überwiegen der Interessen des Betroffenen im Sinne der Nr. 3 liegt dann vor, wenn eine Verletzung der Interessen des Betroffenen ohne Weiteres erkennbar ist. Eine intensive Einzelfallprüfung wird der verantwortlichen Stelle hier aber nicht auferlegt.[1107]

§ 28 Abs. 3 bis 4 BDSG regelt die Verarbeitung oder Nutzung personenbezogener Daten für Zwecke des Adresshandels oder der Werbung, Abs. 6 bis 9 das Erheben, Verarbeiten und Nutzen personenbezogener Daten im Sinne des § 3 Abs. 9 BDSG. § 28a BDSG regelt die Übermittlung personenbezogener Daten an Auskunfteien wie zum Beispiel die SCHUFA.

§ 28b BDSG beschreibt die Zulässigkeitsvoraussetzungen für den Einsatz von Scoring-Werten zum Beispiel bei der Kreditvergabe. § 29 BDSG beschreibt Anforderungen an die geschäftsmäßige Datenerhebung und -verarbeitung insbesondere durch Auskunfteien und Adresshändler.

Aufsichtsbehörden

Zuständig für die Kontrolle der Einhaltung der Bestimmungen der Datenschutzgesetze des Bundes und der Länder sind für den öffentlichen Bereich die Datenschutzbeauftragten des Bundes (§§ 21 bis 26 BDSG) und der Länder. Die Aufsicht über den privaten Sektor wird gemäß § 38 Abs. 6 BDSG durch die Aufsichtsbehörden der Länder ausgeübt. Diese sind teilweise die Landesdatenschutzbeauftragten, teilweise sind sie in den Innenministerien oder Regierungspräsidien angesiedelt. Die Aufsichtsbehörden

1104 Taeger, in: Taeger / Gabel 2010, § 28 BDSG, Rn. 30 ff.
1105 Gola / Schomerus 2010, § 28 BDSG, Rn. 24.
1106 Taeger, in: Taeger / Gabel 2010, § 28 BDSG, Rn. 80 ff.
1107 Simitis, in: Simitis 2011, § 28 BDSG, Rn. 162 f.

können einerseits von Amts wegen, andererseits auf Anrufung durch Bürger hin aktiv werden. Ihre Aufsichtsrechte umfassen insbesondere Zutrittsrechte zu Dienst- und Geschäftsräumen, Auskunftsrechte, sowie Einsichtsrechte bezüglich Daten und Unterlagen (§§ 24 Abs. 4 und 38 Abs. 4 BDSG sowie entsprechende Vorschriften in Landesdatenschutzgesetzen). Während der Bundesbeauftragte für den Datenschutz gemäß § 25 BDSG Datenschutzverstöße gegenüber den jeweils übergeordneten Stellen nur beanstanden kann, können die Aufsichtsbehörden für den privaten Bereich gemäß § 38 Abs. 5 BDSG Maßnahmen zur Verbesserung des Datenschutzes anordnen, in schweren Fällen die weitere automatisierte Datenverarbeitung untersagen und die Abberufung des betrieblichen Datenschutzbeauftragten verlangen, wenn dieser nicht über die notwendige Fachkunde verfügt. Als weitere Einwirkungsmöglichkeiten gegen Datenschutzverstöße stehen das Bußgeld- und Strafverfahren nach den Vorschriften der §§ 43 und 44 BDSG zur Verfügung.

5.4.3 BEREICHSSPEZIFISCHE REGELUNGEN

5.4.3.1 Telekommunikationsdatenschutz

Anwendungsbereich des Telekommunikationsgesetzes

Die Datenschutzregeln der §§ 91 ff. TKG sind anwendbar auf den Umgang mit personenbezogenen Daten der Nutzer von Telekommunikationsdiensten durch geschäftsmäßige Anbieter solcher Dienste. Geschäftsmäßig in diesem Sinne handeln gemäß § 3 Nr. 10 TKG alle Anbieter, die mit oder ohne Gewinnerzielungsabsicht Telekommunikationsdienste nachhaltig anbieten. Der Begriff *„geschäftsmäßig"* ist hier also nicht mit dem Begriff *„gewerbsmäßig"* zu verwechseln, bei dem es auf eine Gewinnerzielungsabsicht ankommt. Das entscheidende Merkmal der Nachhaltigkeit bedeutet eine auf Dauer angelegte Diensterbringung, womit auch die Behörden, Schulen, Krankenhäuser, Hotels und andere Stellen mit eigenem Telekommunikationsnetz in den Anwendungsbereich des § 91 Abs. 1 Satz 1 TKG einbezogen werden.[1108] Sie gehören allerdings dann nicht zu den Diensteanbietern im Sinne der Vorschrift, wenn sie die Nutzung ihrer Netzte nur zu rein dienstlichen Zwecken erlauben. Die private Nutzung durch Beschäftigte wird daher bei den nicht gewerbsmäßigen Dienstebetreibern oft untersagt, um nicht den Datenschutzregeln des Telekommunikationsgesetzes zu unterliegen.[1109] Das Bundesdatenschutzgesetz und die Landesdatenschutzgesetze sind gegenüber den §§ 91 ff. TKG nur subsidiär anwendbar, also dort, wo dieses selbst keine Regelung trifft.

Verarbeitungsschritte

Im Telekommunikationsgesetz (wie auch im Telemediengesetz) werden anstatt der Bezeichnung der Datenverarbeitungsschritte mit *„erheben"*, *„verarbeiten"* und *„nutzen"* die Begriffe *„erheben"* und *„verwenden"* benutzt. Ein inhaltlicher Unterschied ist darin jedoch nicht enthalten.

Informationspflichten

Gemäß § 93 TKG haben Diensteanbieter ihre Teilnehmer schon bei Vertragsschluss über Art, Umfang, Ort und Zweck der Erhebung und Verwendung personenbezogener Daten sowie über ihre Wahl- und Gestaltungsmöglichkeiten zu unterrichten. Weitergehende Informationspflichten nach dem Bundesdatenschutzgesetz bleiben gemäß § 93 Abs. 1 Satz 4 TKG bestehen.

Elektronische Einwilligung

Gemäß § 94 TKG kann die datenschutzrechtliche Einwilligung, die grundsätzlich gemäß § 4a Abs. 1 BDSG schriftlich erklärt werden muss, im Anwendungsbereich des Telekommunikationsgesetzes unter besonderen Voraussetzungen auch elektronisch erklärt werden. Der Dienstanbieter muss hierbei sicherstellen, dass der Teilnehmer seine Einwilligung bewusst und eindeutig erteilt hat. Die Einwilligung ist überdies zu protokollieren, damit die Teilnehmer jederzeit

1108 Eckhardt, in: Spindler / Schuster 2011, § 88 TKG, Rn. 16 f.
1109 Eckhardt, in: Spindler / Schuster 2011, § 88 TKG, Rn. 18.

einsehen können, wann und in welchem Umfang sie eingewilligt haben. Die Teilnehmer müssen die Einwilligung jederzeit mit Wirkung für die Zukunft widerrufen können.

Erlaubnisnormen

Die Erlaubnisnormen des Telekommunikationsgesetzes unterscheiden zwischen Bestandsdaten und Verkehrsdaten.

Bestandsdaten sind gemäß § 3 Nr. 3 TKG Daten eines Teilnehmers, die für die Begründung, inhaltliche Ausgestaltung, Änderung oder Beendigung eines Vertragsverhältnisses über Telekommunikationsdienste erhoben werden, insbesondere Name, Anschrift, Kontoverbindung und Art des Vertrags.[1110] Gemäß § 95 Abs. 1 TKG dürfen Bestandsdaten erhoben werden, soweit sie zu den in § 3 Nr. 3 TKG genannten Zwecken erforderlich sind. Abs. 2 regelt die Nutzung von Bestandsdaten zu Werbezwecken, die hauptsächlich für die gewerbsmäßigen Diensteanbieter von Interesse sein dürften. Gemäß Abs. 3 sind die Bestandsdaten bei Beendigung des Vertragsverhältnisses bis zum Ablauf des folgenden Kalenderjahres zu löschen. Gemäß § 95 Abs. 5 TKG darf die Erbringung eines Telekommunikationsdienstes nicht von einer Einwilligung zur Datenverwendung abhängig gemacht werden (Kopplungsverbot), wenn für den Telekommunikationsdienst eine Monopolstellung besteht.

Verkehrsdaten sind gemäß § 3 Nr. 30 solche Daten, die bei der Erbringung eines Telekommunikationsdienstes erhoben, verarbeitet oder genutzt werden. Hierzu gehören die Rufnummern von Anrufer und Angerufenem, Datum, Uhrzeit und Dauer der Verbindung sowie Art des Telekommunikationsdienstes.[1111] Die Erhebung und Verwendung von Verkehrsdaten ist in § 96 TKG eng begrenzt. Gemäß § 96 Abs. 1 TKG dürfen die in den Nummern 1 bis 5 genannten Verkehrsdaten erhoben und verwendet werden, soweit dies für die im Abschnitt 2 des 7. Teils des TKG genannten Zwecke erforderlich ist. Nach Nr. 1 dürfen gespeichert werden: Die Nummer oder Kennung der beteiligten Anschlüsse, personenbezogene Berechtigungserkennungen, bei Kundenkarten auch die Kartennummer, bei mobilen Anschlüssen die Standortdaten. Hierunter sind grundsätzlich auch IP-Adressen zu zählen. Nach Nr. 2 dürfen Beginn und Ende der jeweiligen Verbindung nach Datum und Uhrzeit und, soweit die Entgelte davon abhängen, die übermittelten Datenmengen erhoben und verwendet werden. Zahlen die Nutzer Pauschalsummen (Flatrates), sind die Datenmengen für die Entgeltermittlung nicht erforderlich.

Über das Ende der Verbindung hinaus dürfen Verkehrsdaten gemäß § 95 Abs. 2 TKG nur verwendet werden, soweit sie zum Aufbau weiterer Verbindungen, zur Entgeltermittlung oder -abrechnung oder für die in §§ 100 und 101 TKG genannten Zwecke erforderlich sind. Anderenfalls sind sie gemäß § 96 Abs. 2 Satz 2 TKG nach Beendigung der Verbindung unverzüglich, also ohne schuldhaftes Zögern, zu löschen.

§ 93 Abs. 3 TKG erlaubt die Verwendung von Verkehrsdaten für die Vermarktung und bedarfsgerechte Gestaltung von Telekommunikationsdiensten nur unter Einwilligung des Betroffenen. Die Daten der Angerufenen sind unverzüglich zu anonymisieren, sofern nicht auch sie eingewilligt haben. Für diese Einwilligung muss der Betroffene gemäß Abs. 4 über die zu verwendenden Datenarten, die Dauer der Speicherung und sein Recht, die Einwilligung jederzeit zu widerrufen, unterrichtet werden.

§ 97 Abs. 1 Satz 1 TKG erlaubt den Diensteanbietern die Verwendung der erhobenen Verkehrsdaten, soweit dies zur Ermittlung des Entgelts und zur Abrechnung mit den Teilnehmern erforderlich ist. Satz 2 enthält eine Sonderregelung für Anbieter ohne eigenes Netz, um diesen die Abrechnung in gleicher Weise zu ermöglichen. Zusätzlich zu den in § 96 Abs. 1 TKG aufgeführten Verkehrsdaten dürfen die Diensteanbieter gemäß § 97 Abs. 2 Nr. 2 und 3 TKG bestimmte Bestandsdaten und weitere für die Abrechnung

1110 Holznagel / Ricke, in: Spindler / Schuster 2011, § 3 TKG, Rn. 5.
1111 Eckhardt, in: Spindler / Schuster 2011, § 96 TKG, Rn. 2 f.

erhebliche Umstände erheben und verwenden. Gemäß § 97 Abs. 3 TKG müssen die Diensteanbieter unverzüglich nach Beendigung einer Verbindung die für die Entgeltermittlung erheblichen Daten aussondern und nicht mehr erforderliche Daten löschen.

§ 98 TKG enthält Vorschriften über die Datenverwendung beim Angebot standortbezogener Dienste. Die hierfür erforderlichen Standortdaten dürfen nur im erforderlichen Maß und innerhalb des dafür erforderlichen Zeitraums verarbeitet werden und dies auch nur dann, wenn sie anonymisiert werden und die Teilnehmer eingewilligt haben.[1112]

Die Vorschriften in §§ 113a und 113b TKG, die eine anlasslose Speicherung von Verkehrsdaten für sechs Monate vorschrieben und eine Übermittlung für Strafverfolgung, Gefahrenabwehr und Aufgaben der Geheimdienste regelten, sind mit Urteil des Bundesverfassungsgerichts vom 2. März 2010[1113] als nichtig festgestellt worden, da sie gegen das Fernmeldegeheimnis aus Art. 10 Abs. 1 GG verstoßen.[1114] Bis zu einer möglichen Neuregelung besteht im Telekommunikationsgesetz keine Mindestspeicherpflicht für Verkehrsdaten.

5.4.3.2 Datenschutz bei Telemediendiensten

Anwendungsbereich des Telemediengesetzes

Das Telemediengesetz (TMG) wurde im Jahr 2007 erlassen und ersetzte das Teledienstegesetz und das Teledienstedatenschutzgesetz sowie teilweise den Mediendienstestaatsvertrag Die Verantwortlichkeit von Anbietern von Telemediendiensten sowie die für diese geltenden Datenschutzregelungen wurden im Telemediengesetz zusammengeführt. Das Telemediengesetz übernimmt an dieser Stelle weitgehend die Datenschutzregelungen aus dem Teledienstedatenschutzgesetz und dem Mediendienstestaatsvertrag.[1115]

Das Gesetz ist anwendbar auf Telemedien. Diese sind in § 1 Abs. 1 Satz 1 TMG definiert als elektronische Informations- und Kommunikationsdienste, soweit sie nicht Telekommunikation oder Rundfunk sind. Telekommunikation sind gemäß § 3 Nr. 24 TKG Dienste, die *ganz oder überwiegend* in der Übertragung von Signalen über Telekommunikationsnetze bestehen. Insbesondere die Internet-Telefonie stellt damit keinen Telemediendienst, sondern einen Telekommunikationsdienst dar.[1116] Gemäß § 1 Abs. 1 TMG fallen allerdings nur solche Telekommunikationsdienste aus seinem Anwendungsbereich heraus, die *ganz* in der Übertragung von Signalen bestehen. Zum Beispiel Dienste von E-Mail- und Access-Providern, die nicht nur, aber überwiegend Signale transportieren, unterfallen daher mit Ausnahme einiger Datenschutzregelungen[1117] zugleich dem Telekommunikationsgesetz und dem Telemediengesetz. Rundfunk sind gemäß § 2 Rundfunkstaatsvertrag lineare Informations- und Kommunikationsdienste. Sie bestehen aus für die Allgemeinheit bestimmten Veranstaltungen in Ton oder Bild entlang eines Sendeplans, unter Benutzung elektromagnetischer Wellen. Nach der Begründung zum Telemediengesetz sollen zum Rundfunk neben seinen herkömmlichen Formen (Fernsehen und Hörfunk) auch Live-Streaming (zusätzliche zeitgleiche Übertragung herkömmlicher Rundfunkprogramme über das Internet) und Web-Casting (ausschließliche Übertragung herkömmlicher Rundfunkprogramme über das Internet) gehören. Hingegen gehören Radio- und Fernsehtext, Teleshopping und Video-on-Demand zu den Telemedien.[1118] Zu den eindeutigen Telemediendiensten gehören zum Beispiel

1112 Eckhardt, in: Spindler / Schuster 2011, § 98 TKG, Rn. 11 ff.
1113 BVerfGE 125, 260.
1114 Siehe Roßnagel, NJW 2010, S. 544.
1115 Spindler / Nink, in: Spindler / Schuster 2011, § 11 TMG, Rn. 1.
1116 BT-Drs. 16/3078, 13.
1117 Siehe § 11 Abs. 3 TMG.
1118 BT-Drs. 16/3078, 13.

Online-Shops für Waren und Dienstleistungen mit direkter Bestellmöglichkeit, Online-Presse, Chatrooms, Suchdienste, Soziale Netzwerke und Werbe-Mails.[1119]

Gemäß § 1 Abs. 2 TMG gilt das Telemediengesetz und gelten damit dessen Datenschutzregeln sowohl für private als auch für öffentliche Stellen, unabhängig davon, ob die Nutzung entgeltlich oder unentgeltlich erfolgt. Wenn diese auf ihren Webseiten Informationen, Datenbankzugriffe, Suchfunktionen, etc. anbieten, unterliegen sie dabei den Datenschutzregeln der §§ 11 bis 15a TMG. Allerdings gelten diese gemäß § 11 Abs. 1 Nr. 1 TMG dann nicht, wenn die Telemediendienste im Beschäftigungsverhältnis ausschließlich zu dienstlichen Zwecken oder innerhalb oder zwischen privaten oder öffentlichen Stellen ausschließlich zur Steuerung von Arbeits- oder Geschäftsprozessen bereitgestellt werden. Dürfen die Beschäftigten die Telemediendienste jedoch auch zu privaten Zwecken nutzen, sind die Datenschutzregeln für die gesamte Nutzung anzuwenden.[1120]

Datenschutzregeln des Telemediengesetzes

Das Telemediengesetz enthält bereichsspezifische Datenschutznormen, die in ihrem Anwendungsbereich den allgemeinen Regeln des Bundesdatenschutzgesetzes vorgehen. Das Erheben und Verwenden personenbezogener Daten erlaubt § 12 Abs. 1 BDSG den Anbietern von Telemediendiensten nur soweit, wie ein Gesetz oder eine andere Rechtsvorschrift, die sich ausdrücklich auf Telemedien bezieht, es erlaubt oder der betroffene Nutzer eingewilligt hat. Die Einwilligung kann nach § 13 Abs. 2 TMG elektronisch erklärt werden, wobei die Voraussetzungen denen in § 94 TKG entsprechen. Erlaubnisnormen sind in den §§ 14 und 15 TMG für Bestandsdaten, Nutzungsdaten und Abrechnungsdaten enthalten.

Bestandsdaten sind auch im Telemediengesetz Daten, die zur Begründung, Ausgestaltung oder Änderung des Nutzungsvertrags benötigt werden. Sie dürfen gemäß § 14 Abs. 1 TMG erhoben werden, soweit sie im konkreten Fall erforderlich sind. Im Einzelfall darf über Bestandsdaten gemäß § 14 Abs. 2 TMG zur Strafverfolgung und Gefahrenabwehr sowie für die Erfüllung der Aufgaben von Verfassungsschutz, Nachrichtendiensten und Bundeskriminalamt, auch zur Durchsetzung der Rechte am geistigen Eigentum, auf Anordnung der jeweiligen Behörde Auskunft erteilt werden. Hierzu muss der Diensteanbieter nicht besondere Daten speichern, sondern nur das weitergeben, was er zulässigerweise gespeichert hat. Die Umsetzung der Richtlinie zur Vorratsdatenspeicherung, die eine besondere Speicherpflicht begründete, ist durch das Urteil des Bundesverfassungsgerichts[1121] aufgehoben worden.

Nutzungsdaten sind im Telemediengesetz gemäß § 15 Abs. 1 Satz 2 insbesondere: Merkmale zur Identifikation des Nutzers, Angaben über Beginn und Ende sowie des Umfangs der jeweiligen Nutzung und Angaben über die vom Nutzer in Anspruch genommenen Telemedien. Sie dürfen erhoben und verwendet werden, soweit dies zur Ermöglichung der Inanspruchnahme der Dienste erforderlich ist. Gemäß § 15 Abs. 2 TMG darf der Diensteanbieter Nutzungsdaten über die Inanspruchnahme verschiedener Telemedien zusammenführen, soweit dies zur Abrechnung mit dem Nutzer erforderlich ist. Für Zwecke der Werbung, der Marktforschung oder zur bedarfsgerechten Gestaltung darf der Diensteanbieter gemäß § 15 Abs. 3 Satz 1 TMG pseudonymisierte Nutzungsprofile erstellen, sofern der Nutzer nicht widerspricht. Auf das Widerspruchsrecht ist der Nutzer gemäß Satz 2 hinzuweisen.

Abrechnungsdaten sind gemäß § 15 Abs. 4 Satz 1 TMG personenbezogene Daten, die zur Abrechnung mit dem Nutzer erforderlich sind. Sind sie hierzu erforderlich, dürfen Nutzungsdaten über das Ende des Nutzungsvorgangs hinaus verarbeitet und genutzt werden. Soweit zur Ermittlung des Entgelts erforderlich, darf der Diensteanbieter gemäß

1119 Roßnagel, NVwZ 2007, 743.
1120 Spindler / Nink, in: Spindler / Schuster 2011, § 11 TMG, Rn. 11.
1121 BVerfGE 125, 260.

Abs. 5 Satz 1 Abrechnungsdaten an andere Diensteanbieter oder Dritte übermitteln. In anonymisierter Form dürfen die Nutzungsdaten gemäß Abs. 5 Satz 3 auch für die Marktforschung an andere Diensteanbieter übermittelt werden. Auch für Nutzungsdaten gilt gemäß Abs. 5 Satz 4 die Erlaubnis des § 14 Abs. 2, Nutzungsdaten an die dort genannten Behörden und Personen zu übermitteln. Gemäß § 15 Abs. 6 TMG darf eine Abrechnung Zeitpunkt, Dauer, Art, Inhalt und Häufigkeit einer Telemediennutzung nur erkennen lassen, wenn der Nutzer einen Einzelnachweis verlangt. Die Speicherung von Abrechnungsdaten ist gemäß § 15 Abs. 7 TMG zeitlich beschränkt.

Nach § 13 Abs. 1 TMG hat der Diensteanbieter den betroffenen Nutzer zu Beginn der Nutzung des Dienstes über Art, Umfang, Ort und Zwecke der Erhebung, Verarbeitung und Nutzung personenbezogener Daten zu informieren. Auf Webseiten finden sich daher häufig umfangreiche Datenschutzerklärungen.

5.5 MODERNISIERUNGSDISKUSSION

Die Diskussion zur Modernisierung des Datenschutzes läuft bereits seit mehr als einem Jahrzehnt. Die größeren Beiträge sowie aktuelle Gesetzgebungsvorhaben werden in diesem Abschnitt zusammenfassend dargestellt.

5.5.1 GUTACHTEN IM AUFTRAG DES BUNDESINNENMINISTERIUMS 2001

Alexander Roßnagel, Andreas Pfitzmann und Hansjürgen Garstka erstellten 2001 im Auftrag des Bundesministeriums des Innern ein umfassendes Gutachten über eine Modernisierung des Datenschutzrechts.[1122] Das Gutachten enthält weitreichende, insbesondere strukturelle Reformkonzepte für das deutsche Datenschutzrecht. Das Gutachten orientierte sich schon damals an technischen und gesellschaftlichen Entwicklungen, deren andauernde Aktualität im Projekt Internet Privacy zu beachten sein wird. Viele der angesprochenen Problemstellungen wurden bis heute rechtlich nicht gelöst, sodass sich das Gutachten, obwohl es bereits über zehn Jahre alt ist, in weiten Teilen auf der Höhe der Modernisierungsdiskussion befindet.

Zentrale Konzepte zur Modernisierung des Datenschutzrechts sind die rechtliche Regulierung und Durchsetzung von Systemdatenschutz,[1123] die Förderung von Selbstdatenschutz[1124] und das Schaffen von Anreizen für Datenschutz und Datensicherheit bei den verantwortlichen Stellen.[1125] Das Gutachten empfiehlt, den Datenschutz weniger durch zeitlich punktuelle Zulassung einzelner Datenverarbeitungsvorgänge zu verwirklichen als vielmehr durch die Etablierung ständig zu beachtender Gestaltungs- und Verarbeitungsregeln.[1126]

Um den von Datenverarbeitung betroffenen Personen die Wahrnehmung ihrer Rechte zu erleichtern und um das Datenschutzrecht auf hohem Niveau zu konsolidieren, schlägt das Gutachten insbesondere vor, das in viele Spezialgesetze zersplitterte Rechtsgebiet deutlich zu vereinfachen. Es soll in einem neuen Bundesdatenschutzgesetz gebündelt werden, das nicht mehr grundsätzlich subsidiär, sondern primär Anwendung finden soll, und somit eine klarere Struktur erhalten.[1127] Dieses neue Gesetz soll sich an den fortschrittlichsten Datenschutzgesetzen aus dem Telekommunikations- und Telemedienbereich orientieren. Die Aufspaltung in Regelungen für den öffentlichen und den nicht öffentlichen Bereich soll aufgegeben und durch

1122 Roßnagel / Pfitzmann / Garstka 2001.
1123 Roßnagel / Pfitzmann / Garstka 2001, S. 39 f.
1124 Roßnagel / Pfitzmann / Garstka 2001, S. 40 ff.
1125 Roßnagel / Pfitzmann / Garstka 2001, S. 42.
1126 Roßnagel / Pfitzmann / Garstka 2001, S. 70 ff.
1127 Roßnagel / Pfitzmann / Garstka 2001, S. 43.

einheitliche und risikoadäquate Lösungen für die Datenverarbeitung in beiden Bereichen ersetzt werden. Auch die Unterscheidung zwischen automatisierter und manueller Datenverarbeitung soll aufgegeben werden.[1128]

Überdies wird vorgeschlagen, das Datenschutzrecht durch eine Stärkung der Rolle der Einwilligung und eine gesetzlich regulierte Selbstregulierung von der bisherigen *„Normenflut"* zu befreien. Um hierbei die Selbstbestimmung der Betroffenen zu wahren und zu fördern, muss aber die Freiwilligkeit des datenschutzrechtlich relevanten Handelns abgesichert werden.[1129] Das Gutachten setzt darauf, die Ziele des Datenschutzrechts nicht lediglich durch administrative Instrumente durchzusetzen, sondern sie auch durch Kooperation mit den verantwortlichen Stellen und die Förderung eines Wettbewerbs um den besten Datenschutz zwischen ihnen zu erreichen.[1130]

Das Gutachten schlägt überdies vor, die informationelle Selbstbestimmung als *„Grundrecht der Informationsgesellschaft"* in das Grundgesetz aufzunehmen. Hierdurch würde die Rechtsprechung des Bundesverfassungsgerichts durch den Verfassungsgesetzgeber ausdrücklich anerkannt und die besondere Bedeutung des Datenschutzes in der Informationsgesellschaft herausgestellt. Das Grundrecht soll aber nicht rein persönlichkeitsrechtlich gefasst werden, sondern als Kommunikationsgrundrecht in Verbindung mit den anderen Kommunikationsgrundrechten die *„verfassungsrechtliche Grundlage einer umfassenden Informations- und Kommunikationsordnung"* bilden. Der objektivrechtliche Gehalt der informationellen Selbstbestimmung könnte in dieser Hinsicht durch die Aufnahme in den Grundrechtskatalog vor allem für den nicht öffentlichen Bereich, den ihr Abwehrcharakter kaum betrifft, hervorgehoben und strukturiert werden. Die verfassungsrechtliche Kodifizierung der informationellen Selbstbestimmung[1131] sieht das Gutachten aber unabhängig von den übrigen Modernisierungsvorschlägen und nicht als Bedingung für diese.[1132]

Das Gutachten konkretisiert die allgemeinen Konzepte in vielerlei Hinsicht. Die für das Projekt Internet Privacy wichtigsten Punkte werden im Folgenden ausgeführt:

Ein modernisiertes Bundesdatenschutzgesetz soll neben der Gefahrenabwehr auch Risikovorsorge treffen. Das Gutachten schlägt vor, auch bezüglich solcher Daten, die zum Zeitpunkt ihrer Erhebung nicht personenbezogen oder personenbeziehbar sind, Vorsorge zu betreiben, um den Personenbezug auch in der Zukunft möglichst weitgehend zu begrenzen.[1133]

Das Gutachten spricht sich dafür aus, den Schutz des Bundesdatenschutzgesetzes von personenbezogenen Daten natürlicher Personen auf Daten juristischer Personen auszuweiten. Sie weisen darauf hin, dass juristische Personen zwar keines Schutzes bei der menschenwürdebezogenen Persönlichkeitsentfaltung bedürfen. Zum einen gehe aber die informationelle Selbstbestimmung über diesen Bereich hinaus und sei insofern gemäß Art. 19 Abs. 3 GG auch auf juristische Personen anzuwenden. Zum anderen sei Schutzgut des Bundesdatenschutzgesetzes neben der informationellen Selbstbestimmung auch das auf juristische Personen anwendbare Telekommunikationsgeheimnis. Der Telekommunikationsdatenschutz sei daher auch gerade nicht auf natürliche Personen beschränkt. Überdies seien in anderen Datenschutzregelungen, zum Beispiel § 35 Abs. 4 SGB I, Betriebs- und Geschäftsgeheimnisse den Daten natürlicher Personen gleichgestellt. Eine allgemeine Angleichung stelle daher eine Harmonisierung des

1128 Roßnagel / Pfitzmann / Garstka 2001, S. 44.
1129 Roßnagel / Pfitzmann / Garstka 2001, S. 44.
1130 Roßnagel / Pfitzmann / Garstka 2001, S. 45.
1131 Siehe zu dieser auch Roßnagel 2009, S. 99 ff.
1132 Roßnagel / Pfitzmann / Garstka 2001, S. 57 f.
1133 Roßnagel / Pfitzmann / Garstka 2001, S. 61.

Datenschutzrechts dar. Überdies sei eine Unterscheidung ohnehin oft schwer möglich, da Daten juristischer Personen in der Regel auch Daten zu natürlichen Personen enthalten. Insbesondere Publizitäts-, Unterrichtungs-, Auskunfts-, und Informationspflichten der juristischen Personen dürften aber durch eine solche Erstreckung des Datenschutzrechts in keiner Weise berührt werden.[1134]

Personenbezogene Daten und ihre Verarbeitung sollen in drei Stufen gewichtet werden. Der Umgang mit besonders schützenswerten Daten soll besonderen Schutz erfahren. Der Umgang mit Daten, bei denen aufgrund der Offenkundigkeit der Daten schützenswerte Interessen Betroffener offensichtlich nicht entgegenstehen, sowie Erhebung und Speicherung von Daten aus frei zugänglichen Quellen sollen grundsätzlich zulässig sein. Zwischen diesen beiden Extremen liegen *„normale"* personenbezogene Daten, für deren Verarbeitung grundsätzlich Einwilligungen oder Erlaubnistatbestände notwendig sind.[1135]

Das Gutachten ist der Ansicht, der Begriff der *„verantwortlichen Stelle"* sei im Bundesdatenschutzgesetz zu eng definiert. Verantwortliche Stelle ist nach § 3 Abs. 7 BDSG jede Person oder Stelle, die personenbezogene Daten für sich selbst verarbeitet oder nutzt oder dies durch andere vornehmen lässt. Da es in einer „vernetzten Welt allgegenwärtiger Datenverarbeitung" eine stetig wachsende Anzahl an der Datenverarbeitung Beteiligter gibt und geben wird, bestehe bei diesem Begriff das Risiko, dass nicht alle Teilschritte der Datenverarbeitung von ihm erfasst würden. Daher solle stattdessen der weitere Begriff aus Art. 2 lit. d) der EU-Datenschutzrichtlinie übernommen werden, der die verantwortliche Stelle nicht anhand der Verarbeitung, sondern anhand der Entscheidung über Zweck und Mittel der Datenverarbeitung bestimmt.[1136]

Es wird vorgeschlagen, anstatt vieler einzelner Verarbeitungsschritte für jeden Umgang mit personenbezogenen Daten einheitlich den Begriff der *„Datenverarbeitung"* zu verwenden, wie dies auch in der Datenschutzrichtlinie der Fall ist, um jeden Umgang, auch mögliche zukünftige Umgangsformen abzudecken.[1137] Dabei soll aber unterschieden werden zwischen Daten, die gezielt personenbezogen verarbeitet werden und solchen Daten, die zunächst anonym verarbeitet werden, bei denen aber in Zukunft ein Personenbezug entstehen kann. An diese beiden Verarbeitungsformen sollen unterschiedliche Anforderungen gestellt werden. Während für die gezielt personenbezogen verarbeiteten Daten die allgemeinen Anforderungen gelten sollen, soll die nicht gezielt personenbezogene Datenverarbeitung generell zugelassen werden, wenn die Daten einer strengen Zweckbindung unterliegen und nach Zweckerreichung umgehend gelöscht werden. In diese Kategorie werden zum Beispiel Daten gerechnet, die bei der technischen Weiterleitung oder Aufbereitung oder als unbeabsichtigte Treffer einer Suchanfrage anfallen. Diese differenzierte Herangehensweise entspreche dem Umstand, dass in Zukunft immer mehr Handlungen in der realen Welt Datenspuren hinterlassen werden und immer mehr Daten benötigt werden, um die Dienste der Zukunft zu erbringen. Soweit es der verarbeitenden Stelle nicht auf den Personenbezug ankomme und durch Löschung nach Erreichen des Zwecks das Risiko des Personenbezugs ausgeschlossen oder bedeutend gemindert werde, sei es effizienzsteigernd und risikoadäquat, die Verarbeitung allgemein zuzulassen.[1138] Für die nicht gezielt personenbezogene Datenverarbeitung soll keine individuelle Unterrichtung des Betroffenen verlangt werden, sondern eine allgemeine Datenschutzerklärung ausreichen, zumal die Datenverarbeitung für die Betroffenen nur ein geringes Risiko darstellt und die verarbeitende Stelle häufig gar nicht wissen wird, *„wessen"* Daten sie ungezielt verarbeitet.[1139]

1134 Roßnagel / Pfitzmann / Garstka 2001, S. 64 ff.
1135 Roßnagel / Pfitzmann / Garstka 2001, S. 61 f.
1136 Roßnagel / Pfitzmann / Garstka 2001, S. 63.
1137 Roßnagel / Pfitzmann / Garstka 2001, S. 67 f.
1138 Roßnagel / Pfitzmann / Garstka 2001, S. 68 ff.
1139 Roßnagel / Pfitzmann / Garstka 2001, S. 85.

Der Einwilligung als grundlegender Ausdruck informationeller Selbstbestimmung sei im privatrechtlichen Bereich Vorrang einzuräumen gegenüber abstrakt-generellen Erlaubnistatbeständen, deren Weite die Zulässigkeit personenbezogener Datenverarbeitung nicht einschränke, sondern in breitem Umfang ermögliche. Im nicht öffentlichen Bereich soll die Einwilligung zur „Hauptlegitimationsgrundlage der Datenverarbeitung"[1140] werden und somit grundsätzlich eine Opt-in-Lösung etabliert werden. Da die Einwilligung damit im privaten Bereich zur Hauptermächtigungsgrundlage der Datenverarbeitung werde, sei es besonders wichtig, dass die Selbstbestimmung bei der Einwilligung nicht bloß formal, sondern faktisch sichergestellt werde. Als Voraussetzung für die Wirksamkeit einer Einwilligung, deren Vorliegen im Zweifelsfall von der verarbeitenden Stelle nachzuweisen wäre, führt das Gutachten unter anderem an: Eine vollständige und verständliche Unterrichtung über die Datenverarbeitung, die genauso weit reicht wie der Anwendungsbereich der Einwilligung, eine tatsächliche Freiwilligkeit, die einen jederzeitigen Widerruf für die Zukunft einschließt, ein Kopplungsverbot zwischen Einwilligung und zumindest Leistungen der zivilisatorischen Grundversorgung.[1141]

Im Bereich öffentlicher Datenverarbeitung ist die Einwilligung hingegen an den Bedürfnissen der jeweiligen Behörde im Rahmen ihrer Aufgabenerfüllung auszurichten. Die Behörden dürfen den Rahmen der zu dieser Aufgabenerfüllung notwendigen Daten grundsätzlich auch nicht durch Einwilligungen erweitern.[1142] Für den öffentlichen Bereich soll ein einheitlicher Erlaubnistatbestand zur Datenverarbeitung statt der vielen bereichsspezifischen Regelungen geschaffen werden, soweit diese nicht besondere Regelungen einführen, sondern lediglich die Grundregeln des Bundesdatenschutzgesetzes wiederholen.[1143]

Zur weiteren Voraussetzung der Datenverarbeitung soll eine möglichst weitgehend anonyme oder pseudonyme Verarbeitung werden. Zusätzlich seien Vorsorgemaßnahmen und wiederholte Neuprognosen notwendig, um den Personenbezug der Daten auch nach der ersten Verarbeitung möglichst weitgehend auszuschließen.[1144]

Entgegen Art. 6 Abs. 1 lit. b) DSRL soll die Erforderlichkeit der Datenverarbeitung für den gegebenen Zweck weiterhin als Zulässigkeitsvoraussetzung erhalten bleiben und nicht die bloße Vereinbarkeit mit dem Zweck genügen. Ansonsten würde für den nicht öffentlichen Bereich die begrenzende Kraft der Einwilligung, im öffentlichen Bereich die der Erlaubnistatbestände geschwächt. Das Verbot der Datensammlung auf Vorrat müsse auch weiterhin, außer in wenigen Ausnahmefällen und dann unter zusätzlichen Sicherungen, gelten.[1145]

Bezüglich einer Bildung von Profilen aus personenbezogenen Daten ist das Gutachten der Ansicht, ein vollständiges Verbot der Profilbildung gehe zu weit, da die Nutzung von Profilen häufig im Interesse des Betroffenen liegen kann. So erlauben es Profile, langwierige Registrierungsprozesse zu beschleunigen und individuell zugeschnittene Dienstleistungen in Anspruch zu nehmen. Die Profilbildung soll stattdessen aufgrund ihrer besonderen Risiken für die informationelle Selbstbestimmung als spezifische Form der Datenverarbeitung streng zweckgebunden und nur gemäß ausdrücklicher Einwilligung oder bei Erfüllung der Voraussetzungen eines Erlaubnistatbestandes zulässig sein.[1146] In § 15 Abs. 3 TMG wird bereits die Profilbildung als spezifische Form der Verarbeitung von Nutzerdaten bereits geregelt.

1140 Roßnagel / Pfitzmann / Garstka 2001, S. 73.
1141 Roßnagel / Pfitzmann / Garstka 2001, S. 91 ff.
1142 Roßnagel / Pfitzmann / Garstka 2001, S. 71 ff.
1143 Roßnagel / Pfitzmann / Garstka 2001, S. 74 ff.
1144 Roßnagel / Pfitzmann / Garstka 2001, S. 102 ff.
1145 Roßnagel / Pfitzmann / Garstka 2001, S. 111 f.
1146 Roßnagel / Pfitzmann / Garstka 2001, S. 117 ff.

Die Datenverarbeitungssysteme sollen transparenter werden, um die Selbstbestimmung der Betroffenen und die Datenschutzkontrolle zu fördern. Aufsichtsbehörden und interessierte Nutzer sollen in die Lage versetzt werden, die Art und Weise nachzuvollziehen, wie die technischen Systeme Daten verarbeiten. Hierzu soll langfristig eine Pflicht zur Offenlegung der Quelltexte und Gestaltungswerkzeuge der Programme eingeführt werden. Kurz- und mittelfristig sollen die möglichst weitgehende Nutzung von Open Source-Software und die Prüfung der Quelltexte durch die Aufsichtsbehörden im Vordergrund stehen.[1147]

Bezüglich der Auftragsdatenverarbeitung schlägt das Gutachten zum einen vor, den Auftragnehmer gegenüber den Betroffenen stärker in die Verantwortung zu nehmen. Zwar sei es richtig, dass grundsätzlich der Auftraggeber als verantwortliche Stelle gelte, da dieser aber faktisch die Datenverarbeitung durch den Auftragnehmer kaum kontrollieren könne, sei eine zusätzliche Verantwortlichkeit des Auftragnehmers zu erwägen. Zum anderen sei eine eigene Regelung über die Funktionsübertragung zu treffen, bei der im Gegensatz zur Auftragsdatenverarbeitung die Verantwortung für die Datenverarbeitung vollständig auf den Dienstleister übertragen wird. Um ein Outsourcing der Datenverarbeitung, sowohl als Auftragsdatenverarbeitung als auch als Funktionsübertragung für Geheimnisträger wie Rechtsanwälte oder Ärzte zu ermöglichen, sei § 203 StGB auf die Auftrags- und Funktionsübernehmer zu erstrecken. Auch Zeugnisverweigerungsrechte und Beschlagnahmeschutz müssten diesbezüglich für sie gelten.[1148]

Der Einsatz datenschutzgerechter Technik soll auf verschiedenen Wegen gefördert werden. Einerseits sollen für die Hersteller der Systeme Prüfpflichten bezüglich der Verwirklichung von Datenschutz durch ihre Systeme und dies bezügliche Protokollierungspflichten eingeführt werden. Andererseits sollen Hard- und Software der Systeme bezüglich des Datenschutzes zertifiziert werden. Die Zertifizierung soll freiwillig ausgestaltet, dafür jedoch mit Prüfsiegeln belohnt werden, die die Hersteller zur Werbung verwenden können. Öffentliche Stellen sollen verpflichtet werden, zertifizierte Produkte bei öffentlichen Ausschreibungen zu bevorzugen und selbst möglichst weitgehend zertifizierte Produkte zu verwenden.[1149] In ähnlicher Weise soll durch Auditierung und Zertifizierung die Einrichtung datenschutzgerechter Datenverarbeitungsprozesse bei den verantwortlichen Stellen angeregt werden.[1150]

Das Gutachten empfiehlt, die Möglichkeiten der Betroffenen zum Selbstdatenschutz zu fördern. So soll ein Recht zum anonymen und pseudonymen Handeln als Grundregel für den Persönlichkeitsschutz etabliert werden, wie es in der Offline-Welt ohnehin weitgehend selbstverständlich ist. Den Staat soll bezüglich dieses Rechts eine Infrastrukturverantwortung treffen. Die Regelungen über die elektronische Form im Bürgerlichen Gesetzbuch müssten dahingehend geändert werden, dass bei einer Signatur der Name nicht grundsätzlich anzugeben sei, um ein pseudonymes Handeln zu ermöglichen. Um trotz des Rechts auf anonymes und pseudonymes Handeln die Rechtsverfolgung gegenüber den handelnden Personen weiterhin zu ermöglichen, wird empfohlen, pseudonyme Zertifikate zu verwenden und ein entsprechendes Aufdeckungsverfahren für den Privatrechtsverkehr zu regeln.[1151]

Empfohlen wird auch, die Ausübung von Betroffenenrechten durch verschiedene Maßnahmen zu erleichtern. Unter anderem wird vorgeschlagen, die Ausübung von Auskunftsrechten den Betroffenen auf elektronischem Weg zu ermöglichen und unentgeltliche Beschwerdeverfahren anzubieten.[1152] Das Gutachten empfiehlt überdies,

1147 Roßnagel / Pfitzmann / Garstka 2001, S. 88 ff.
1148 Roßnagel / Pfitzmann / Garstka 2001, S. 124 f.
1149 Roßnagel / Pfitzmann / Garstka 2001, S. 143 ff.
1150 Roßnagel / Pfitzmann / Garstka 2001, S. 132 ff.
1151 Roßnagel / Pfitzmann / Garstka 2001, S. 148 ff.
1152 Roßnagel / Pfitzmann / Garstka 2001, S. 174 ff.

die Schadensersatzpflichten aus §§ 7 und 8 BDSG zu vereinheitlichen, insbesondere die für die Datenverarbeitung durch öffentliche Stellen geltende Gefährdungshaftung und die Haftung für schwerwiegende immaterielle Schäden auf den privaten Bereich zu übertragen. Dies erleichtere den Betroffenen die Geltendmachung von Ansprüchen und entspreche dem Risiko der heutigen Datenverarbeitung durch den nicht öffentlichen Sektor.[1153]

Die Grundsätze der Datenverarbeitung sollen durch organisatorische Maßnahmen der verantwortlichen Stellen abgesichert werden. Diese sollen im Rahmen eines integrierten Datenschutzmanagementsystems dazu verpflichtet werden, einen Datenschutzorganisationsplan und ein Datenschutz- und Datensicherheitskonzept zu erarbeiten, die bereitgehalten werden sollen und der jeweiligen Kontrollstelle bei Kontrollen auszuhändigen wären. Diese Pläne sollen gebündelt die Informationen darüber enthalten, wer für welche Aufgaben des Datenschutzes verantwortlich ist, welche Daten verarbeitet werden, wie das Datenverarbeitungssystem aufgebaut ist und ein Konzept, welche Risiken für die informationelle Selbstbestimmung durch die Datenverarbeitung bestehen und wie der Datenschutz und die Datensicherheit verwirklicht werden sollen.[1154]

Eine konkretisierende regulierte Selbstregulierung sieht das Gutachten als weiteren wichtigen Ansatz zur Verwirklichung des Datenschutzes im nicht öffentlichen Bereich an. Die Selbstregulierung könne Datenschutzrecht nicht ersetzen, sie könne aber durch branchenspezifische Konkretisierung der gesetzlichen Tatbestandsmerkmale den Gesetzgeber bezüglich der Regelungstiefe entlasten, für eine der Geschwindigkeit der technischen Entwicklung angemessene Flexibilität sorgen und den verantwortlichen Stellen Sicherheit bezüglich der Auslegung gesetzlicher Normen geben. Die Selbstregulierung hätte insofern reguliert zu sein, dass sie nicht zu einer Rechtszersplitterung führen dürfe. So dürften gesetzliche Regeln zwar konkretisiert, aber nicht verändert werden. Um einer einseitigen Interessendurchsetzung in der Selbstregulierung entgegenzuwirken, müssten Verfahren festgelegt werden, die anerkannte Datenschutz- und Verbraucherverbände und die Kontrollstellen in die Konkretisierung der Regelungen einbinden.[1155]

Bezüglich der Datenschutzkontrolle empfiehlt das Gutachten, insbesondere die Kontrolle des öffentlichen und nicht öffentlichen Sektors zusammenzulegen. Darüber hinaus sei die weitere Befreiung der Kontrollstellen aus der Rechtsaufsicht durch die Ministerialverwaltung zu empfehlen, da durch sie die zu kontrollierende Verwaltung die Kontrollstellen selbst kontrolliere.[1156]

5.5.2 DATENSCHUTZ IN EINEM INFORMATISIERTEN ALLTAG 2007

In seinem Gutachten „Datenschutz in einem informatisierten Alltag"[1157] unterbreitet *Alexander Roßnagel* einige spezifische Modernisierungsvorschläge für das Datenschutzrecht angesichts der sich immer stärker abzeichnenden Entwicklung zur allgegenwärtigen Datenverarbeitung. Das Gutachten kommt zu dem Ergebnis, wenn die Datenverarbeitung in Zukunft mehr und mehr in den Hintergrund trete, automatisch und unbemerkt ablaufe, so müsse dies auch für einen entsprechenden wirksamen Datenschutz gelten. Die informationelle Selbstbestimmung müsse überall und jederzeit ausgeübt werden können, automatisierbar werden und sei durch Infrastrukturmaßnahmen zu unterstützen. Ein eigenes Datenschutzgesetz für Ubiquitous Computing sei nicht zielführend. Vielmehr müsse die Fortentwicklung des

1153 Roßnagel / Pfitzmann / Garstka 2001, S. 179 ff.
1154 Roßnagel / Pfitzmann / Garstka 2001, S. 131 f.
1155 Roßnagel / Pfitzmann / Garstka 2001, S. 131 f.
1156 Roßnagel / Pfitzmann / Garstka 2001, S. 153 ff.
1157 Roßnagel 2007.

Datenschutzrechts in das unter oben vorgestellte Modernisierungskonzept eingebettet werden.[1158]

Gegenüber dem Gutachten von 2001 sind hier vor allem die Abschnitte über die datenschutzrechtliche Einwilligung von Interesse. Die im Modernisierungsgutachten aus 2001 empfohlene Opt-in-Lösung, die die Datenverarbeitung im nicht öffentlichen Bereich grundsätzlich von der Einwilligung des Betroffenen abhängig werden ließe, sei zwar richtig. Sie sei aber für die allgegenwärtige Datenverarbeitung und der einhergehenden Vielzahl von Datenverarbeitungen selbst in der elektronischen Form des § 13 Abs. 2 TMG nicht zu bewältigen und würde eine völlige Überforderung der Betroffenen mit sich bringen. Die Einwilligung könne in der Welt allgegenwärtiger Datenverarbeitung nur in generalisierter Form erhalten bleiben.[1159] Sie müsse hierzu auf technische Datenschutzsysteme „delegiert" werden, die nach den Präferenzen des Betroffenen voreingestellt wären und die Nutzung von Diensten automatisiert anhand dieser Präferenzen auswählen könnten. Daneben müsse es auch als Einwilligung des Betroffenen gelten, wenn er ein Datenverarbeitungssystem bewusst und freiwillig auswählt und dabei die Möglichkeit hat, die Datenschutzfunktionen des Systems für sich zu konfigurieren.[1160]

Der Vorschlag aus dem Modernisierungsgutachten, Datenschutz stärker durch zu beachtende Gestaltungs- und Verarbeitungsregeln als durch jeweils einmalige Zulassung von Datenverarbeitungen zu gewährleisten,[1161] wird aufgegriffen und für die allgegenwärtige Datenverarbeitung spezifiziert. Verarbeitungs- und Gestaltungsregeln können zwar von den Dienstanbietern durch auditierte Datenschutzmanagementsysteme und umfassende Datenschutzerklärungen offengelegt werden. Damit sie aber die Selbstbestimmung der Nutzer erhöhen, müssten sie auch von diesen in angemessener Weise wahrgenommen werden können. Da dies aber bei der allgegenwärtigen und häufig unbemerkten Nutzung zahlloser Dienste im Alltag eine völlige Überforderung der Nutzer bedeuten würde, müssten die Dienste es technisch ermöglichen, dass automatisierte Datenschutzagenten die Dienste gemäß der Präferenzen des Nutzers anhand der Gestaltungs- und Verarbeitungsregeln aussuchen.[1162]

Im Gegensatz zum Modernisierungsgutachten[1163] wird es nicht mehr für risikoadäquat angesehen, die rein persönliche und familiäre Datenverarbeitung weiterhin vollständig vom Datenschutzrecht ausgenommen zu belassen. Aufgrund der fortschreitenden *„informationstechnischen Aufrüstung"* des Einzelnen hätten sich die Grundlagen dieser Privilegierung grundlegend verschoben. Eine vollständige Anwendung des Datenschutzrechts sei aber ebenfalls unangemessen. Aufgrund der inzwischen auch von der persönlichen Datenverarbeitung ausgehenden Risiken für die informationelle Selbstbestimmung sei aber zu diskutieren, welche einzelnen Regelungen zur Beherrschung dieser Risiken geeignet seien. Er nennt diesbezüglich als Vorschläge insbesondere das Datengeheimnis aus § 5 BDSG, die Schadensersatzregelung aus § 7 BDSG, die Regelungen über die Datensicherung in § 9 BDSG sowie die Regelungen zur Auftragsdatenverarbeitung aus § 11 BDSG.[1164]

Angesichts der Möglichkeit, mit Daten aus der allgegenwärtigen Datenverarbeitung potentiell vollständige Alltagsprofile der Nutzer zusammenzutragen, werde zum einen eine informationelle Gewaltenteilung immer bedeutender und zum anderen das Verbot der Datensammlung auf Vorrat immer wichtiger. Eine informationelle Gewaltenteilung sei durch die verschiedenen Diensteanbieter zunächst zwar gegeben, sodass die Betroffenen den Fluss ihrer Daten noch

1158 Roßnagel 2007, S. 175 f.
1159 Roßnagel 2007, S. 136 ff.
1160 Roßnagel 2007, S. 179.
1161 Roßnagel / Pfitzmann / Garstka 2001, S. 70 ff.
1162 Roßnagel 2007, S. 179 ff.
1163 Roßnagel / Pfitzmann / Garstka 2001, S. 61.
1164 Roßnagel 2007, S. 192 ff.

einigermaßen rollenbasiert nachvollziehen können. Diese Trennung dürfe allerdings nicht durch weitreichende rollenübergreifende Kontrollbefugnisse der Strafverfolgungs- und Gefahrenabwehrbehörden und der Nachrichtendienste aufgelöst werden. Insgesamt sei es angesichts des Kontrollpotentials der allgegenwärtigen Datenverarbeitung für den Schutz der informationellen Selbstbestimmung von hoher Bedeutung, derartige Eingriffsbefugnisse der Sicherheitsbehörden als Ausnahmefälle und nicht als alltäglich zu konzipieren. Die Befugnisse für den Normalfall seien auch am Risikopotential des normalen Alltags und nicht am extremen Ausnahmefall zu orientieren.[1165]

Für die Zukunft müsse gewährleistet werden, dass Räume und Zeiten verbleiben, die frei von allgegenwärtiger Datenverarbeitung sind und dass kein Anschluss- und Nutzungszwang entstehe. Durch ein Kopplungsverbot müsse zumindest für wichtige Infrastrukturleistungen auch eine Nutzung ohne gleichzeitige Nutzung allgegenwärtiger Datenverarbeitung möglich bleiben.[1166]

Datenschutz sei in einer Welt allgegenwärtiger Datenverarbeitung weniger durch Befehle, sondern eher durch Anreize für die verarbeitenden Stellen und Hersteller von Systemen zu erreichen. Den Anbietern datenschutzgerechter Technik müssten Wettbewerbsvorteile, zum Beispiel in Form werbewirksamer Zertifikate, angeboten werden. Das Recht müsse die geeigneten Rahmenbedingungen schaffen, damit sich ein Wettbewerb um den besten Datenschutz entwickle.[1167]

5.5.3 GESETZENTWURF ZUM BESCHÄFTIGTENDATENSCHUTZ 2010

Mit Gesetzentwurf vom 15.12.2010 hat die Bundesregierung einen Vorschlag zur Neuregelung des Beschäftigtendatenschutzes[1168] in den Bundestag eingebracht. Eine Entscheidung des Gesetzgebers über den Entwurf steht bisher noch aus. Der Entwurf enthält Regelungen zu einem Bereich, der für das Projekt Internet Privacy interessant ist, namentlich zur Recherche von Arbeitgebern über Bewerber und Beschäftigte im Internet und insbesondere in sozialen Netzwerken. § 32 Abs. 6 des BDSG-E soll laut dem Gesetzentwurf wie folgend gefasst werden:

> „Beschäftigtendaten sind unmittelbar bei dem Beschäftigten zu erheben. Wenn der Arbeitgeber den Beschäftigten vor der Erhebung hierauf hingewiesen hat, darf der Arbeitgeber allgemein zugängliche Daten ohne Mitwirkung des Beschäftigten erheben, es sei denn, dass das schutzwürdige Interesse des Beschäftigten an dem Ausschluss der Erhebung das berechtigte Interesse des Arbeitgebers überwiegt. Bei Daten aus sozialen Netzwerken, die der elektronischen Kommunikation dienen, überwiegt das schutzwürdige Interesse des Beschäftigten; dies gilt nicht für soziale Netzwerke, die zur Darstellung der beruflichen Qualifikation ihrer Mitglieder bestimmt sind. Mit Einwilligung des Beschäftigten darf der Arbeitgeber auch bei sonstigen Dritten personenbezogene Daten des Beschäftigten erheben; dem Beschäftigten ist auf Verlangen über den Inhalt der erhobenen Daten Auskunft zu erteilen. Die Absätze 1 bis 5 sowie § 32a BDSG-E bleiben unberührt."

§ 32 BDSG-E bezieht sich insgesamt auf Datenverarbeitung vor Begründung eines Beschäftigungsverhältnisses, sodass trotz der Bezeichnung *„Beschäftigtendaten"*, die sowohl für die Daten von Bewerbern als auch für die von bereits Beschäftigten verwendet wird, hier zunächst nur *Bewerber*daten gemeint sind. Der zweite Satz sieht eine Ausnahme zum Direkterhebungsgrundsatz vor und erlaubt

1165 Roßnagel 2007, S. 188 ff.
1166 Roßnagel 2007, S. 191.
1167 Roßnagel 2007, S. 194 f.
1168 BT-Drs. 17/4230.

es, allgemein zugängliche Daten, also auch im Internet frei verfügbare Daten, ohne Mitwirkung des Beschäftigten zu erheben, soweit er hierüber vorher unterrichtet wird und seine schutzwürdigen Interessen am Ausschluss einer Erhebung nicht überwiegen. Für im Internet frei verfügbare Daten außerhalb sozialer Netzwerke müsste also eine Abwägung im Einzelfall vorgenommen werden.

Satz 3 konkretisiert das schutzwürdige Interesse auf die Datenerhebung aus sozialen Netzwerken. Bei Daten aus Netzwerken, die der Kommunikation dienen, überwiegt das Interesse des Betroffenen am Ausschluss der Datenerhebung. Eine Ausnahme gilt lediglich für soziale Netzwerke, die der Darstellung der beruflichen Qualifikation dienen. Im *laufenden Beschäftigungsverhältnis* kann der Arbeitgeber Beschäftigtendaten nach § 32c BDSG-E erheben, soweit dies zur Durchführung, Beendigung oder Abwicklung des Beschäftigungsverhältnisses erforderlich ist. Dies ist unter anderem gemäß Abs. 1 Satz 2 Nr. 3 auch zur Leistungs- und Verhaltenskontrolle möglich. Hierbei gilt § 32 Abs. 6 BDSG-E dann entsprechend. Die Erhebung zur Verhaltens- und Leistungskontrolle aus normalen sozialen Netzwerken ist also auch hier gesperrt. Die in soziale Netzwerke, die nicht der Darstellung der beruflichen Qualifikation dienen, eingestellten Beschäftigtendaten wären damit nach dem Gesetzentwurf der Erhebung durch den Arbeitgeber, grundsätzlich entzogen. Auch durch eine Einwilligung des Beschäftigten könnte hiervon aufgrund der in § 32l Abs. 1 BDSG-E enthaltenen Sperre nicht abgewichen werden.

Verarbeiten und nutzen darf der Arbeitgeber Beschäftigtendaten vor und während des Beschäftigungsverhältnisses gemäß §§ 32b und 32d BDSG-E nur, wenn er sie in zulässiger Weise gemäß §§ 32, 32a BDSG-E beziehungsweise §§ 32, 32a oder 32c BDSG-E erhoben hat oder sie nach diesen Vorschriften hätte erheben dürfen. Für Beschäftigtendaten aus gewöhnlichen sozialen Netzwerken ergäbe sich somit eine allgemeine Erhebungs-, Verarbeitungs- und Nutzungssperre. Etwas anderes würde gemäß § 32b Abs. 2 Satz 2 BDSG-E nur dann gelten, wenn der Bewerber solche Daten dem Arbeitgeber aus eigenem Antrieb übermittelt.

Eine praktische Auswirkung der Regelungen wird allerdings trotz ihrer Klarheit bezweifelt, da der Nachweis eines Verstoßes kaum zu führen sei.[1169]

5.5.4 VORSCHLAG DER KONFERENZ DER DATENSCHUTZBEAUFTRAGTEN DES BUNDES UND DER LÄNDER 2010

Im März 2010 hat die Konferenz der Datenschutzbeauftragten des Bundes und der Länder ein Eckpunktepapier „Ein modernes Datenschutzrecht für das 21. Jahrhundert"[1170] vorgelegt. Auch die Datenschutzbeauftragten diskutieren eine Modernisierung des Datenschutzrechts mit Blick auf die Risiken, die die allgegenwärtige Datenverarbeitung und das globale Internet für das informationelle Selbstbestimmungsrecht bereithalten. Dabei konzentrieren sie sich auf den Menschenwürdegehalt des Grundrechts und fordern, Ausgangspunkt für das Datenschutzrecht müsse der einzelne Mensch und dessen Schutz sein. Diese eigentliche Zielsetzung trete trotz der wiederholten Hervorhebung seiner Bedeutung durch das Bundesverfassungsgericht immer stärker in den Hintergrund.[1171] Vorgeschlagen wird insbesondere, das Datenschutzrecht deutlich zu vereinfachen, ihm einen technikneutralen Ansatz zu verleihen, konkrete, für jede Datenverarbeitung geltende Schutzziele einzuführen, die Betroffenenrechte zu stärken, das Datenschutzrecht auf das Internet zuzuschneiden, die Datenschutzaufsicht zu stärken und die Sanktionsmöglichkeiten zu auszubauen.[1172] Insgesamt zeigt sich eine weitgehende Übereinstimmung mit dem

1169 Heinson / Sörup / Wybitul, CR 2010, S. 753.
1170 Konferenz der Datenschutzbeauftragten des Bundes und der Länder 2010.
1171 Konferenz der Datenschutzbeauftragten des Bundes und der Länder 2010, S. 6 f.
1172 Konferenz der Datenschutzbeauftragten des Bundes und der Länder 2010, S. 3 f.

Gutachten von *Roßnagel*, *Pfitzmann* und *Garstka*,[1173] dessen Forderungen damit unter Datenschutzexperten immer noch als aktuell gelten.

Der datenschutzrechtliche Schutz für Minderjährige soll dadurch verbessert werden, dass klare Regelungen eingeführt werden, unter welchen Voraussetzungen Minderjährige datenschutzrechtlich einwilligen können, da der Minderjährigenschutz des Bürgerlichen Gesetzbuchs nicht immer greife und die Grundrechtsfähigkeit nicht mit einem bestimmten Alter beginne.[1174]

Als besonders aktuelles Problemgebiet greifen die Datenschutzbeauftragten die grenzüberschreitende Datenverarbeitung durch verschiedene Stellen im Rahmen des Cloud Computing auf. Weder das Konzept der Auftragsdatenverarbeitung noch die Datenübermittlung im Rahmen einer Funktionsübertragung halten sie für in der Praxis durchführbar beziehungsweise interessengerecht. Daher sei zum einen das Konzept datenschutzrechtlicher Verantwortlichkeit neu zu regeln und zu erweitern, zum anderen seien besondere Anforderungen für die gemeinsame Datenverarbeitung durch verschiedene Stellen notwendig.[1175] Neben einer Erweiterung des § 203 StGB auf die Auftragnehmer, um Berufsgeheimnisträgern die Nutzung von IT-Dienstleistungen zu ermöglichen, halten die Datenschutzbeauftragten eine spezifische Norm zur Auftragsdatenverarbeitung in Drittländern für notwendig, die sich am Datenschutzniveau des jeweiligen Landes orientiert.[1176]

Auch die Datenschutzbeauftragten setzen verstärkt auf einen Datenschutz durch Technik und Organisation. Sie fordern eine Modernisierung der Anlage zu § 9 BDSG anhand der IT-Schutzziele[1177] Verfügbarkeit, Vertraulichkeit, Integrität, Transparenz und Nichtverkettbarkeit. Als zusätzliches Schutzziel schlagen sie die *„Intervenierbarkeit"* vor, die die technische Ausgestaltung von Betroffenenrechten bedeuten soll. Die Risiken für die informationelle Selbstbestimmung durch ein Datenverarbeitungsverfahren sollen vor dessen Freigabe untersucht und durch ein entsprechendes Sicherheitskonzept behoben oder gemindert werden. Risikoanalyse und Sicherheitskonzept seien regelmäßig nach dem Stand der Technik fortzuschreiben.[1178] Datenvermeidung und Datensparsamkeit sollen gegenüber der bisherigen Zielvorgabe in § 3a BDSG in verbindlicher und sanktionierter Form konkretisiert werden.[1179]

Weiterhin sollen die Betroffenenrechte gestärkt werden. Dies geschieht zum einen durch eine Ausweitung der Informationspflichten der verantwortlichen Stellen. Die Verantwortlichkeit für die Datenverarbeitung müsse klar und eindeutig erkennbar sein und Kerninformationen über die Datenverarbeitung stets an prominenter Stelle platziert werden anstatt versteckt in mehrseitigen Einwilligungserklärungen. Zum anderen fordern die Datenschutzbeauftragten die Einführung einfacher elektronischer Auskunftsverfahren.[1180]

Da die Einwilligung besonders in der Welt allgegenwärtiger Datenverarbeitung als Ermächtigungsgrundlage eine zentrale Rolle einnehme, sei die Freiwilligkeit der Einwilligungen gegenüber faktischen Zwangslagen abzusichern. Einwilligungen sollen nur durch aktives Handeln und nur noch mit begrenzter Geltungsdauer möglich sein, da die Betroffenen ansonsten die Konsequenzen der Einwilligung nicht überblicken könnten. Der Widerruf einer Einwilligung soll für die Betroffenen nur gegenüber der

1173 Siehe oben.
1174 Konferenz der Datenschutzbeauftragten des Bundes und der Länder 2010, S. 8 f.
1175 Konferenz der Datenschutzbeauftragten des Bundes und der Länder 2010, S. 14 ff.
1176 Konferenz der Datenschutzbeauftragten des Bundes und der Länder 2010, S. 16 f.
1177 So auch Roßnagel / Pfitzmann / Garstka 2001, S. 192.
1178 Konferenz der Datenschutzbeauftragten des Bundes und der Länder 2010, S. 18 ff.
1179 Konferenz der Datenschutzbeauftragten des Bundes und der Länder 2010, S. 9 f.
1180 Konferenz der Datenschutzbeauftragten des Bundes und der Länder 2010, S. 21.

ersten datenverarbeitenden Stelle notwendig sein, die ihn an alle folgenden Stellen zu übermitteln haben soll. Das Kopplungsverbot müsse über den Kreis marktbeherrschender Unternehmen ausgeweitet werden.[1181]

Die Datenschutzbeauftragten fordern eine Anpassung des Datenschutzrechts an das globale Internet. Die nationale Gesetzgebung sei durch internationale Vereinbarungen mit dem Ziel eines möglichst hohen internationalen Datenschutzniveaus zu flankieren. Unter vielen spezifischen Regelungsvorschlägen für das Internet sticht die Forderung nach Verfallsdaten für im Internet veröffentlichte personenbezogene Daten hervor, die von Suchmaschinen und anderen Dienstanbietern zu beachten sein sollen.[1182] Überdies sei zu überdenken, inwiefern im Internet veröffentlichte personenbezogene Daten weiterhin unter geringeren Anforderungen verarbeitet werden dürften. Hier sei einerseits der Begriff der öffentlich zugänglichen Daten einzuschränken, andererseits bedürfe es spezieller Regelungen bezüglich der Interessenabwägung und der Zweckbindung bei solchen Datenverarbeitungen.[1183]

Auch die Datenschutzbeauftragten sprechen sich für eine einheitliche Gefährdungshaftung öffentlicher und nicht öffentlicher Stellen bei unzulässiger Datenverarbeitung aus.[1184] Sie erweitern dies um die Forderung nach einem pauschalierten Schadensersatzanspruch für immaterielle Schäden, um den Betroffenen die Last der Bezifferung der Anspruchshöhe abzunehmen. Übermitteln Stellen unrichtige Daten, soll gegen diese ein Anspruch auf Beseitigung der Folgen der Übermittlung eingeführt werden.[1185]

Darüber hinaus unterbreiten die Datenschutzbeauftragten eine Reihe von Vorschlägen für die Effektivierung der Datenschutzkontrolle. Beispielsweise sollen die kontrollierten Stellen zur Mitwirkung an den Kontrollen verpflichtet werden, da die Kontrollbehörden ihre Arbeit nicht durchführen könnten, wenn vor Ort niemand Fragen beantwortet oder die Datenverarbeitungssysteme erläutert. Dem Bundesbeauftragten soll ein Anordnungsrecht eingeräumt werden. Die Kontrollbehörden sollen eine Strafantragsbefugnis gemäß § 205 StGB erhalten. Den Staatsanwaltschaften soll die Möglichkeit eröffnet werden, bei datenschutzrechtlichen Straftaten, die von besonderem öffentlichem Interesse sind, von Amts wegen zu ermitteln. Hierzu ist bisher ein Antrag notwendig. Die datenschutzrechtlichen Bußgeldtatbestände sollen erweitert werden, insbesondere um die Unterlassung organisatorischer und technischer Datenschutzmaßnahmen. Die Informationspflicht bei Datenpannen soll auf öffentliche Stellen erweitert werden.[1186]

5.5.5 REFORMVORSCHLÄGE DER EUROPÄISCHEN KOMMISSION VOM 25.1.2012

Am 25.1.2012 legte die Europäische Kommission weitreichende Reformvorschläge für ein einheitliches Datenschutzrecht in der Europäischen Union vor. Dieses Reformpaket besteht aus einer Grundverordnung für den Datenschutz,[1187] die die bisherige Datenschutzrichtlinie ablösen soll, und einer Richtlinie für den Datenschutz im Bereich der Strafverfolgung und Gefahrenabwehr.[1188] Für

1181 Konferenz der Datenschutzbeauftragten des Bundes und der Länder 2010, S. 22 f.
1182 Konferenz der Datenschutzbeauftragten des Bundes und der Länder 2010, S. 24 ff.
1183 Konferenz der Datenschutzbeauftragten des Bundes und der Länder 2010, S. 35.
1184 Siehe schon oben Roßnagel / Pfitzmann / Garstka 2001.
1185 Konferenz der Datenschutzbeauftragten des Bundes und der Länder 2010, S. 31 f.
1186 Konferenz der Datenschutzbeauftragten des Bundes und der Länder 2010, S. 29 f.
1187 „Vorschlag für Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutz-Grundverordnung)", Brüssel 25.1.2012, KOM (2012) 11 endg.
1188 „Vorschlag für Richtlinie des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Aufdeckung, Untersuchung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr", Brüssel 25.1.2012, KOM (2012) 10 endg.

den Datenschutz im Internet ist vor allem der Entwurf einer Verordnung (DSGVO-E) von Interesse. Im Gegensatz zur bisherigen Richtlinie würde die Verordnung unmittelbare Geltung in allen Mitgliedstaaten erlangen und weite Bereiche der nationalen Datenschutzgesetzgebung verdrängen.[1189]

Dies gilt allerdings nicht für den Regelungsbereich, der von der Richtlinie 2002/58/EG zum Datenschutz in der elektronischen Kommunikation erfasst ist. Denn nach Art. 89 Abs. 1 DSGVO-E werden den Anbietern elektronischer Kommunikationsdienste in öffentlichen Kommunikationsnetzen durch die vorgeschlagene Verordnung keine zusätzlichen Pflichten auferlegt, soweit sie besonderen Pflichten aus der Richtlinie unterliegen, die dasselbe Ziel verfolgen. Dies würde bedeuten, dass die Datenschutzregeln für Telekommunikationsanbieter in §§ 91 ff. TKG, die auf der Richtlinie beruhen, weiterhin als bereichsspezifische Regelungen anwendbar blieben.[1190] Die Einbeziehung juristischer Personen in den Betroffenenkreis in § 91 Satz 2 TKG, die sich im Verordnungsentwurf nicht findet, bliebe damit erhalten. Dies gilt jedoch nicht für die Datenschutzregelungen der §§ 11 ff. TMG und die allgemeinen Vorschriften in §§ 28 ff. BDSG. Diese würden aufgrund des Anwendungsvorrangs der Datenschutz-Grundverordnung unanwendbar. Im Folgenden wird daher insbesondere dargestellt, ob und wenn ja welchen Ersatz für die verdrängten Vorschriften der Verordnungsentwurf bereithält. Zusätzlich werden einige für den Datenschutz im Internet besonders relevante Regelungen herausgegriffen.

Gemäß Art. 3 Abs. 1 DSGVO-E ist die Verordnung dann anwendbar, wenn der für die Verarbeitung Verantwortliche oder der Auftragsverarbeiter seine Tätigkeit im Rahmen einer Niederlassung innerhalb der Europäischen Union ausübt. Eine Niederlassung ist dabei jede feste Einrichtung, von der eine effektive und tatsächliche Ausübung der Tätigkeit vorgenommen wird. Außerdem wäre europäisches Recht immer dann anwendbar, wenn personenbezogene Daten bei einer in der Union ansässigen natürlichen Person erhoben werden, um ihr Waren oder Dienstleistungen anzubieten oder ihr Verhalten zu beobachten – auch wenn keine Niederlassung in der Europäischen Union besteht. Dadurch wird der Anwendungsbereich des europäischen Datenschutzrechts ausgeweitet und die Wahrnehmung von Betroffenenrechten erleichtert. Nutzerfreundlicher wäre es jedoch, einheitlich für jede Form der Datenverarbeitung auf den Sitz der betroffenen Person abzustellen.

Sachlich hält der Verordnungsentwurf gemäß Art. 2 Abs. 2 d) DSGVO-E daran fest, rein persönliche und familiäre Datenverarbeitungen aus seinem Anwendungsbereich auszuschließen. Insofern wird die Forderung nach einer zumindest partiellen Einbeziehung im Lichte der allgegenwärtigen Datenverarbeitung[1191] nicht aufgenommen.

Der Verordnungsentwurf hält an der Notwendigkeit einer gesetzlichen Erlaubnis für die Datenverarbeitung fest. Die Erlaubnistatbestände sind abschließend in Art. 6 DSGVO-E aufgelistet. Die Datenverarbeitung ist zulässig, wenn eine Einwilligung der betroffenen Person vorliegt (lit. a) oder die Verarbeitung der Erfüllung eines Vertrags (lit. b), einer gesetzlichen Verpflichtung (lit. c) oder lebenswichtigen Interessen der betroffenen Person (lit. d) dient. Sie ist außerdem erlaubt, wenn sie für Aufgaben im öffentlichen Interesse (lit. e) oder zur Wahrung berechtigter Interessen des Verantwortlichen (lit. f) erforderlich ist. Zwischen Adressaten aus dem öffentlichen oder privaten Bereich sowie der Verarbeitung zu eigenen Geschäftszwecken und zur Übermittlung wird, anders als bisher im BDSG, nicht mehr differenziert.[1192]

Der Erlaubnistatbestand des berechtigten Interesses erlaubt die Datenverarbeitung, wenn Interessen der betroffenen Person nicht überwiegen. Um diese äußerst unscharfe

1189 Übersichten zum Verordnungsentwurf bei Hornung, ZD 2012, 99; Lang, K&R 2012, 145; Eckhardt, CR 2012, 195.
1190 Eckhardt, CR 2012, 196.
1191 Roßnagel 2007, S. 192 ff.
1192 Eckhardt, CR 2012, 197.

Regelung in ihrem Ausmaß einzuschränken und ein gewisses Maß an Transparenz zu schaffen, ist gemäß Art. 14 Abs. 1 DSGVO-E das berechtigte Interesse gegenüber der betroffenen Person offenzulegen und sie auf ihr Widerspruchsrecht hinzuweisen.[1193] Die nähere Ausgestaltung wird dabei der Europäischen Kommission überlassen, die in delegierten Rechtsakten verschiedene Bereiche und Verarbeitungssituationen festlegen kann.

Die in §§ 14 und 15 TMG getroffene Differenzierung zwischen Bestands-, Nutzungs- und Inhaltsdaten und die einhergehende gesetzliche Bindung des Datenumgangs an bestimmte Zwecke würde mit der Verordnung entfallen. Diese Differenzierung sorgt bisher für einen demokratisch legitimierten Interessenausgleich zwischen den Grundrechten der Internetnutzer und den Bedürfnissen der Anbieter bei der Bereitstellung ihrer Dienste. Übrig bliebe mit Art. 6 DSGVO-E eine weich und weit formulierte Erlaubnisvorschrift, die weit hinter der derzeit geltenden deutschen Rechtslage zurückbleibt. Damit würde eine hohe Rechtsunsicherheit bei der Erhebung und Verarbeitung von personenbezogenen Daten im Internet herbeigeführt.

Der Verordnungsentwurf hält Neuerungen für die datenschutzrechtliche Einwilligung bereit. Die Einwilligung muss freiwillig sein. Ausgeschlossen wäre eine wirksame Einwilligung gemäß Art. 7 Abs. 4 DSGVO-E dann, wenn zwischen der betroffenen Person und dem für die Verarbeitung Verantwortlichen ein erhebliches Ungleichgewicht besteht. Exemplarisch genannt, aber keinesfalls abschließend, sind in Erwägungsgrund 34 DSGVO-E Beschäftigungsverhältnisse aufgrund ihres Abhängigkeitscharakters.

Eine Einwilligung von Kindern soll nach Art. 8 Abs. 1 Satz 1 DSGVO-E nur wirksam sein, wenn sie bereits das dreizehnte Lebensjahr vollendet haben. Sind sie jünger, soll zusätzlich die Zustimmung der Eltern oder des Vormunds des Kindes erforderlich sein. Gemäß Art. 8 Abs. 1 Satz 2 DSGVO-E hat der für die Verarbeitung Verantwortliche unter Berücksichtigung vorhandener Technologie angemessene Anstrengungen zu unternehmen,[1194] um nachprüfbare Einwilligungen zu erhalten. Die Vorschrift dürfte einen großen Anteil der Internetangebote betreffen, vor allem Social Networks, Gemäß Art. 8 Abs. 2 DSGVO-E lässt Abs. 1 das allgemeine Vertragsrecht der Mitgliedstaaten unangetastet. Daher ändert sich nichts an dem Problem, dass die Nutzungsverträge von Minderjährigen mit den Diensteanbietern gemäß §§ 106, 107 BGB ebenfalls häufig nicht wirksam sein werden und hierdurch als Grundlage für eine zulässige Datenverarbeitung gemäß Art. 6 b) DSGVO-E entfielen.[1195] Ein Altersverifikationssystem und eine Zustimmungsmöglichkeit gemäß § 182 Abs. 2 BGB müssten daher bezüglich der Minderjährigen über dreizehn Jahren vorgehalten werden, um wirksame Nutzungsverträge mit ihnen zu schließen, auf die dann die Befugnis zur Datenverarbeitung gemäß Art. 6 Abs. 1 b) DSGVO-E gestützt werden könnte.[1196]

Die Wirksamkeit einer Einwilligung soll nicht von ihrer Schriftform abhängig sein, doch trägt der Diensteanbieter gemäß Art. 7 Abs. 1 DSGVO-E die Beweislast für die Einwilligung, sodass er auf eine Protokollierung nicht verzichten kann. Damit wird sich an der derzeitigen Situation wenig ändern, nach der gemäß § 13 Abs. 2 TMG eine elektronische Einwilligung möglich ist, die vom Diensteanbieter zu protokollieren ist.[1197]

In Art. 40 ff. DSGVO-E zentral geregelt würde die Übermittlung personenbezogener Daten in Drittländer. Zulässig wäre diese zum einen, wenn die Kommission einen Angemessenheitsbeschluss gemäß Art. 41 DSGVO-E erlässt, in dem festgestellt wird, dass das Drittland einen angemessenen Schutz der personenbezogenen Daten bietet. Zum anderen

1193 So auch Lang, K&R 2012, 147.
1194 Kritisch Hornung, ZD 2012, 99 (S. 103), der hierin eine Abschwächung der Beweislastregel in Art. 7 Abs. 1 DSGVO-E sieht.
1195 Jandt / Roßnagel, MMR 2011, 637 (S. 639 f.).
1196 Jandt / Roßnagel, MMR 2011, 637 (S. 640).
1197 Hornung, ZD 2012, 99 (S. 102 f.)

wäre die Übermittlung zulässig, wenn der für die Verarbeitung Verantwortliche geeignete Garantien zum Schutz personenbezogener Daten in Form eines rechtsverbindlichen Instruments vorgesehen hat. Inhaltlich ändert sich nichts, lediglich die Zuständigkeit wird von den Mitgliedsstaaten auf die Kommission übertragen. Das zwischen der EU und den USA bestehende Datenschutzabkommen (Safe Harbor), das die Übermittlung personenbezogener Daten in die USA seit dem Jahr 2000 regelt, wird gemäß Erwägungsgrund 79 DSGVO-E auch in Zukunft bestehen bleiben.

Der Verordnungsentwurf verfolgt das Ziel, der betroffenen Person umfassende Transparenz bei der Datenverarbeitung zu gewährleisten. Hierfür soll der Verantwortliche gemäß Art. 11 Abs. 1 DSGVO-E eine nachvollziehbare und für jedermann leicht zugängliche Strategie verfolgen. Wichtig ist dabei, die elektronische Ausübung der Rechte zu ermöglichen[1198] sowie gemäß Art. 11 Abs. 2 DSGVO-E und Erwägungsgrund 46 eine adressatengerechte Sprache zu verwenden, besonders wenn die Information an Kinder gerichtet ist. Eine ausreichende Transparenz soll – wie bisher im deutschen Recht – vor allem durch eine umfassende Information des Betroffenen und durch ein Auskunftsrecht erreicht werden.

Groß herausgestellt hat die Kommission das *„neue"* Recht auf Vergessenwerden in Art. 17 DSGVO-E. Besonderes Augenmerk wird dabei auf Daten gelegt, die die betroffene Person im Kindesalter öffentlich gemacht hat. Zusätzlich zur bisherigen Regelung eine Anspruchs auf Datenlöschung soll der Verantwortliche, sofern er die von ihm erhobenen Daten öffentlich gemacht hat, alle vertretbaren Schritte unternehmen, um Dritte, die diese Daten verarbeitet haben, darüber zu informieren, dass die betroffene Person die Löschung sämtlicher Querverweise, Replikationen, Kopien oder ähnliches verlangt hat. Dies ist im deutschen Recht in §§ 20 Abs. 8, 35 Abs. 7 BDSG bereits als Pflicht des Verantwortlichen geregelt. Die bisher unter dem Schlagwort *„Recht auf Vergessenwerden"* diskutierten Löschungs- und Anonymisierungskonzepte[1199] finden sich in Art. 17 DSGVO-E trotz der Überschrift gar nicht wieder. Die Regelung muss insofern als enttäuschendes Blendwerk bezeichnet werden.

Das Recht auf Datenübertragbarkeit gemäß Art. 18 DSGVO-E soll der betroffenen Person nicht nur das Recht geben, eine Kopie ihrer Daten zur weiteren Verwendung zu erhalten, sondern auch, diese Daten in ein anderes Verarbeitungssystem zu überführen, und dem Verantwortlichen damit gleichzeitig die Daten zu entziehen. *„Entziehen"* bedeutet hier aufgrund von Art. 17 Abs. 4 d) nicht zwangsweise *„Löschen"*, denn in diesem Fall ist auch das *„Beschränken"* der weiteren Verarbeitung ausreichend. Der Anwendungsbereich soll gemäß Erwägungsgrund 55 vor allem bei Social Networks liegen, um eine bessere Kontrolle über die eigenen Daten zu ermöglichen. Art. 18 setzt ein entsprechend strukturiertes elektronisches Format voraus, das von der Kommission im Wege eines Durchführungsrechtsaktes festgelegt werden kann. Die Umsetzbarkeit dieses Rechts wird im entscheidenden Maße von diesem Durchführungsrechtsakt abhängen. Neben den bekannten datenschutzrechtlichen Betroffenenrechten wirkt das Recht auf Datenübertragbarkeit wie ein Fremdkörper, denn es ermöglicht besseren Datenschutz allenfalls als Beiprodukt, etwa wenn ein Nutzer hierdurch leichter in ein datenschutzfreundlicheres Social Network abwandert. Das Recht auf Datenübertragbarkeit ist aber in erster Linie kein Recht auf Daten*schutz*, sondern ein Recht auf Daten*mobilität* und folgt aus dem in Art. 1 Abs. 1 DSGVO-E niedergelegten Schutz des freien Verkehrs personenbezogener Daten.

Schließlich hat eine natürliche Person gemäß Art. 20 DSGVO-E das Recht, keinerlei Maßnahmen unterworfen zu werden, die auf einer automatisierten Verarbeitung personenbezogener Daten beruhen und rechtliche Wirkungen für sie entfaltet oder sie in maßgeblicher Weise beeinträchtigt und deren Zweck in der Auswertung bestimmter Merkmale der Person, etwa berufliche oder

1198 So bereits Roßnagel / Pfitzmann / Garstka 2001, S. 170; Hornung, ZD 2011, 51.
1199 Zum Beispiel Nolte, ZRP 2011, 236.

wirtschaftliche Leitungsfähigkeit, persönliche Vorlieben, der Gesundheitszustand oder Ähnliches, besteht (Profiling). Hat die Person eingewilligt, oder dient das Profiling der Erfüllung eines Vertrags, ist eine solche Maßnahme zulässig. Die Empfehlung des – nicht verbindlichen – Erwägungsgrundes 58, Kinder generell nicht solchen Maßnahmen zu unterwerfen, findet sich in Art. 20 DSGVO-E allerdings nicht wieder.

Eingeschränkt werden können die Betroffenenrechte unter den in Art. 21 DSGVO-E genannten Voraussetzungen, zum Beispiel zum Schutz der öffentlichen Sicherheit und Interessen der Union und Mitgliedstaaten, zur Verhütung und Aufdeckung von Straftaten und Verstößen gegen berufsständische Regeln.

Das Datenschutzrecht hat in Deutschland durch mehrere Jahrzehnte der Gesetzgebung, Rechtsprechung und wissenschaftlichen Bearbeitung eine ausgefeilte Systematik erhalten. Die Differenzierung der im Internet anfallenden Daten in Bestands-, Nutzungs- und Inhaltsdaten entsprechende Verarbeitungsvorschriften und angepasste Regelungen eines Datenschutzes durch Technik werden mit der Verordnung verloren gehen. Dies wird für das elaborierte und differenzierte deutsche Datenschutzrecht einen Rückschritt bedeuten. Der Verordnungsentwurf bewegt sich sowohl technologiepolitisch als auch regelungsmethodisch unterhalb des in Deutschland bereits erreichten Niveaus. Die wenigen Verbesserungen im Bereich der elektronischen Betroffenenrechte vermögen dieses Defizit nicht auszugleichen. Ein wesentlicher Beitrag zur Modernisierung des Datenschutzrechts ist von dem Verordnungsentwurf nicht zu erwarten.

Im Gegenteil - der Verordnungsentwurf enthält eine sehr weitgehende *Ent*mächtigung der Mitgliedstaaten im Bereich des Datenschutzes und eine extrem weitgehende *Er*mächtigung der mit geringer demokratischer Legitimation ausgestatteten Kommission. Diese behält sich in zahlreichen Reglungen das Recht vor, die entscheidende inhaltliche Ausfüllung oder Konkretisierung der sehr weit gefassten Normen der Verordnung selbst vorzunehmen. Eine Zentralisierung der Datenschutzrechtsetzung auf Jahrzehnte bei der hierzu auch fachlich nicht ausgestatteten EU-Kommission wird der dynamischen Entwicklung der Informationstechnik nicht gerecht werden und würde dringende Datenschutzinnovationen in den Mitgliedstaaten auf lange Zeit ausbremsen. Insbesondere lässt die Verordnung es nicht zu, dass differenzierte Suchprozesse nach geeigneten Lösungen auf die heute noch unbekannten Probleme der Zukunft in den einzelnen Mitgliedstaaten erfolgen. In einer Situation dynamischer Entwicklung und vielfältiger, aber unbekannter Herausforderungen ist die vorgesehene Zentralisierung der Rechtssetzung allein bei der Kommission evolutorisch die falsche Strategie.

Eine als Mindestniveau verstandene Richtlinie wäre hier das adäquatere Mittel. Sie könnte in bestimmten Bereichen eine Harmonisierung enthalten, wenn diese tatsächlich notwendig erscheint. Eine verbindliche Vollharmonisierung wäre aus Sicht des deutschen Datenschutzrechts aber nicht nur bezüglich des Datenschutzniveaus ein Rückschritt. Die Frage, wie wir in der Informationsgesellschaft der Gegenwart und Zukunft leben wollen, würde nach dem Willen des Verordnungsgebers nicht mehr von den demokratisch legitimierten Gremien der Mitgliedstaaten, sondern von der Brüsseler Bürokratie und ihrem Lobby-Diskurs entschieden.

LITERATUR

Bergmann / Möhrle / Herb 2011
Bergmann, L. / Möhrle, R. / Herb, A.: *Datenschutzrecht Kommentar*, Stuttgart, Stand: September 2011.

Callies / Ruffert 2011
Callies, C. / Ruffert, M., EUV/EGV: *Das Verfassungsrecht der Europäischen Union mit Europäischer Grundrechtecharta*, 4. Auflage, München 2011 (zitiert als: Bearbeiter, in: Callies/Ruffert 2011).

Dreier 2004
Dreier, H.: *Grundgesetzkommentar*, Band I – Art. 1-19, 2. Auflage, Tübingen 2004 (zitiert als: Bearbeiter, in: Dreier 2004).

Eckardt, CR 2012
Eckhardt, J.: *EU-Datenschutz-VO – Ein Schreckgespenst oder Fortschritt?*, CR 2012, 195.

Jandt 2008
Jandt, S.: *Vertrauen im Mobile Commerce*, Baden-Baden 2008.

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

Gola / Schomerus 2010
Gola, P. / Schomerus, S.: *Bundesdatenschutzgesetz Kommentar*, 10. Auflage, München 2010.

Heinson / Sörup / Wybitul, CR 2010
Heinson, D. / Sörup, T. / Wybitul, T.: *Der Regierungsentwurf zur Neuregelung des Beschäftigtendatenschutzes*, CR 2010, 751.

Hornung, ZD 2011
Hornung, G.: *Datenschutz durch Technik in Europa*, ZD 2011, 51.

Hornung, ZD 2012
Hornung, G.: *Eine Datenschutz-Grundverordnung für Europa?*, ZD 2012, 99.

Konferenz der Datenschutzbeauftragten des Bundes und der Länder 2010
Konferenz der Datenschutzbeauftragten des Bundes und der Länder, *Ein modernes Datenschutzrecht für das 21. Jahrhundert*, Stuttgart 2010.

Lang, K&R 2012
Lang, M.: *Reform des EU-Datenschutzrechts*, K&R 2012, 145.

Luhmann 2000
Luhmann, N.: *Vertrauen*, 4. Auflage, Stuttgart 2000.

Mangoldt / Klein / Starck 2010
Mangoldt, H. v. / Klein, F. / Starck, C.: *Kommentar zum Grundgesetz*, Band 1, Präambel, Art. 1-19, 6. Auflage, München 2010 (zitiert als: Bearbeiter, in: Mangoldt/Klein/Starck 2010).

Meyer 2011
Meyer, J.: *Charta der Grundrechte der Europäischen Union*, Kommentar, 3. Auflage, Baden-Baden 2011 (zitiert als: Bearbeiter, in: Meyer 2011).

Moos 2006
Moos, F.: *Datenschutzrecht*, Berlin Heidelberg 2006.

Nolte, ZRP 2011
Nolte, N.: *Zum Recht auf Vergessen im Internet - Von digitalen Radiergummis und anderen Instrumenten*, ZRP 2011, 236.

Ohly, AfP 2011
Ohly, A.: *Verändert das Internet unsere Vorstellung von Persönlichkeit und Persönlichkeitsrecht?*, AfP 2011, 428.

Roßnagel 2003
Roßnagel, A.: *Recht der Multimediadienste*, 4. EL., München 2003 (zitiert als: Bearbeiter, in: Roßnagel 2003).

Roßnagel 2007
Roßnagel, A.: *Datenschutz in einem informatisierten Alltag*, Berlin 2007.

Roßnagel, NVwZ 2007
Roßnagel, A.: *Das Telemediengesetz – Neuordnung für Informations- und Kommunikations-dienste*, NVwZ 2007, 743.

Roßnagel 2008
Roßnagel, A.: „Selbst- oder Fremdbestimmung – die Zukunft des Datenschutzes". In: Roßnagel, A. / Sommerlatte, T. / Winand, U. (Hrsg.): *Digitale Visionen – Zur Gestaltung allgegenwärtiger Informationstechnologien*, Berlin 2008, 123.

Roßnagel 2009
Roßnagel, A.: „Die Zukunft informationeller Selbstbestimmung: Datenschutz ins Grundgesetz und Modernisierung des Datenschutzkonzepts". In: Kritische Justiz: *Verfassungsrecht und gesellschaftliche Realität*, Beiheft 1/2009, 99.

Roßnagel, DuD 2010
Roßnagel, A.: *Das Bundesverfassungsgericht und die Vorratsdatenspeicherung in Europa*, DuD 2010, 544.

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

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

Simitis 2011
Simitis, S.: *Bundesdatenschutzgesetz*, 7. Auflage, Baden-Baden 2011 (zitiert als: Bearbeiter, in: Simitis 2011).

Spindler / Schuster 2011
Spindler, G. / Schuster, F.: *Recht der elektronischen Medien - Kommentar*, 2. Auflage, München 2011 (zitiert als: Bearbeiter, in: Spindler/Schuster 2011).

Taeger / Gabel 2010
Taeger, J. / Gabel, D.: *Kommentar zum BDSG*, Frankfurt. a. M. 2010 (zitiert als: Bearbeiter, in: Taeger/Gabel 2010).

Trute 2003
Trute, H.-H.: „Verfassungsrechtliche Grundlagen". In: Roßnagel, A. (Hrsg.): *Handbuch Datenschutzrecht*, München 2003, 156.

> BISHER SIND IN DER REIHE acatech STUDIE UND IHRER VORGÄNGERIN acatech BERICHTET UND EMPFIEHLT FOLGENDE BÄNDE ERSCHIENEN:

Geisberger, Eva/Broy, Manfred (Hrsg.): *agendaCPS. Integrierte Forschungsagenda Cyber-Physical Systems* (acatech STUDIE), Heidelberg u.a.: Springer Verlag 2012.

Appelrath, Hans-Jürgen/Kagermann, Henning/Mayer, Christoph (Hrsg.): *Future Energy Grid. Migrationspfade ins Internet der Energie* (acatech STUDIE), Heidelberg u.a.: Springer Verlag 2012.

Spath, Dieter/Walter, Achim (Hrsg.): *Mehr Innovationen für Deutschland. Wie Inkubatoren akademische Hightech-Ausgründungen besser fördern können* (acatech STUDIE), Heidelberg u.a.: Springer Verlag 2012.

Hüttl, Reinhard. F./Bens, Oliver (Hrsg.): *Georessource Wasser – Herausforderung Globaler Wandel* (acatech STUDIE), Heidelberg u.a.: Springer Verlag 2012.

acatech (Hrsg.): *Organische Elektronik in Deutschland.* (acatech BERICHTET UND EMPFIEHLT, Nr. 6), Heidelberg u.a.: Springer Verlag 2011.

acatech (Hrsg.): *Monitoring von Motivationskonzepten für den Techniknachwuchs* (acatech BERICHTET UND EMPFIEHLT, Nr. 5), Heidelberg u.a.: Springer Verlag 2011.

acatech (Hrsg.): *Wirtschaftliche Entwicklung von Ausgründungen aus außeruniversitären Forschungseinrichtungen* (acatech BERICHTET UND EMPFIEHLT, Nr. 4), Heidelberg u.a.: Springer Verlag 2010.

acatech (Hrsg.): *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.

acatech (Hrsg.): *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 (Hrsg.): *Mobilität 2020. Perspektiven für den Verkehr von morgen* (acatech BERICHTET UND EMPFIEHLT, Nr. 1), Stuttgart: Fraunhofer IRB Verlag 2006.

> acatech – DEUTSCHE AKADEMIE DER TECHNIKWISSENSCHAFTEN

acatech vertritt die Interessen der deutschen Technikwissenschaften im In- und Ausland in selbstbestimmter, unabhängiger und gemeinwohlorientierter Weise. Als Arbeitsakademie berät acatech Politik und Gesellschaft in technikwissenschaftlichen und technologiepolitischen Zukunftsfragen. Darüber hinaus hat es sich acatech zum Ziel gesetzt, den Wissenstransfer zwischen Wissenschaft und Wirtschaft zu erleichtern und den technikwissenschaftlichen Nachwuchs zu fördern. Zu den Mitgliedern der Akademie zählen herausragende Wissenschaftler aus Hochschulen, Forschungseinrichtungen und Unternehmen. acatech finanziert sich durch eine institutionelle Förderung von Bund und Ländern sowie durch Spenden und projektbezogene Drittmittel. Um die Akzeptanz des technischen Fortschritts in Deutschland zu fördern und das Potenzial zukunftsweisender Technologien für Wirtschaft und Gesellschaft deutlich zu machen, veranstaltet acatech Symposien, Foren, Podiumsdiskussionen und Workshops. Mit Studien, Empfehlungen und Stellungnahmen wendet sich acatech an die Öffentlichkeit. acatech besteht aus drei Organen: Die Mitglieder der Akademie sind in der Mitgliederversammlung organisiert; ein Senat mit namhaften Persönlichkeiten aus Industrie, Wissenschaft und Politik berät acatech in Fragen der strategischen Ausrichtung und sorgt für den Austausch mit der Wirtschaft und anderen Wissenschaftsorganisationen in Deutschland; das Präsidium, das von den Akademiemitgliedern und vom Senat bestimmt wird, lenkt die Arbeit. Die Geschäftsstelle von acatech befindet sich in München; zudem ist acatech mit einem Hauptstadtbüro in Berlin und einem Büro in Brüssel vertreten.

Weitere Informationen unter www.acatech.de

> Die Reihe acatech STUDIE

In dieser Reihe erscheinen die Ergebnisberichte von Projekten der Deutschen Akademie der Technikwissenschaften. Die Studien haben das Ziel der Politik- und Gesellschaftsberatung zu technikwissenschaftlichen und technologiepolitischen Zukunftsfragen.