Re-Setting the Stage for Privacy

A Multi-Layered Privacy Interaction Framework and its Application

LEA SOPHIE AESCHLIMANN, REHANA HARASGAMA, FLAVIUS KEHR, CHRISTOPH LUTZ, VESELINA MILANOVA, SEVERINA MÜLLER, PEPE STRATHOFF, AURELIA TAMÒ

Table of Contents

I. Introduction 2
II. The Multi-Layered Privacy Framework 4
A) Micro-Level: Individuals 6
1. Individual's Privacy Calculus 6
2. Interfering with the Individual's Privacy Decision Making 8
2.1. Privacy-Paradox Dilemma 8
2.2. Psychological Limitations and Irrational Privacy Decisions 9
B) Exo-Level: Organizations 10
1. Individual Privacy 11
2. Institutional Privacy 12
C) Meso-Level: Society 14
1. Culture's Role in Shaping Privacy Expectations 14
2. A Cross-Cultural Comparison of Privacy Concerns 15
D) Macro-Level: State 17
1. Role of Governments 18
2. Privacy as a Fundamental Right and Data Protection Norms 19
III. Interactions between the Layers 20
A) Individual – Organizations 21
B) Individual – Society 24
C) Individual – State 26
D) Organizations – Society 29
E) Organizations – State 31
F) Society – State 33
G) Summary 35
IV. Back to the Future - Concluding Remarks 38
A) From Framework to the Future 38
B) From Framework to Practice 39

I. Introduction

The use of the Internet has constantly spread over the past decades, with 85% of the Swiss population having internet access in 2012.[1] Moreover, the development of smartphones and tablet PCs has rendered todays use of Internet services mobile and ubiquitous. Scholars agree that this evolution, often referred to as the "information age", has fundamentally changed the way we behave – e.g. when collaborating and communicating, shopping, or building relationships. Simultaneously, nearly all Internet services and applications conveniently simplifying everyday life collect and store large amounts of private information, including demographics and personal preferences, health and location data, as well as financial information such as bank accounts and credit card numbers.[2] Further, the (automatic) processing of personal data has become simple and comprehensive, with huge amounts of accessible and exploitable data offering endless opportunities.[3] In this regard, however, the provision of personal information has raised concerns on potential misuse, or loss, of data: In a recent survey, for example, 52% of U.S. citizens stated they feared privacy invasion more than threats from terrorism.[4] Similarly, 87% of Swiss Internet users owning a credit card expressed at least medium concerns with regard to the security of their credit card information.[5]

Against this background, scholars from various fields have increasingly engaged in describing and explaining phenomena related to data privacy in the information age, or *information privacy*. Consequently, different understand-

1 International Telecommunications Union Geneva, Percentage of Individuals using the Internet 2000-2012, retrieved from www.itu.int/en/ITU-D/Statistics/Documents/statistics/2013/Individuals_Internet_2000-2012.xls on 11 July 2014.

2 DAVID L. MOTHERSBAUGH/WILLIAM K. FOXX/SHARON E. BEATTY/SIJUN WANG, Disclosure Antecedents in an Online Service Context: The Role of Sensitivity of Information, Journal of Service Research 2012, 76 ff., 77.

3 H. JEFF SMITH/SANDRA J. MILBERG/SANDRA J. BURKE, Information Privacy: Measuring Individuals' Concerns About Organizational Practices, MIS Quarterly 1996, 167 ff., 168.

4 MICHAEL DIMOCK/CARROLL DOHERTY/ALEC TYSON/DANIELLE GEWURZ, Few See Adequate Limits on NSA Surveillance Program, Pew Research Center, 2013, retrieved from http://www.people-press.org/files/legacy-pdf/7-26-2013%20NSA%20release.pdf on 5 August 2014.

5 The World Internet Project, International Report – Fourth Edition, retrieved from http://www.worldinternetproject.net/_files/_//307_2013worldinternetreport.pdf on 6 August 2014.

ings of the nature of privacy exist, ranging from economic ("privacy as a commodity") and psychological ("privacy as a feeling") to legal ("privacy as a right") and philosophical ("privacy as a state of control") perspectives.[6] Scholars have repeatedly alluded to the multi-dimensionality of the construct. FRANCE BÉLANGER and ROBERT E. CROSSLER, for example, suggested that privacy concerns result from complex interactions on different levels, such as government, society, or the economy, while H. JEFF SMITH and colleagues emphasized the role of culture as a predictor of individual privacy beliefs and attitudes.[7] Still, research referring to a comprehensive understanding of information privacy as a multi-level construct is scarce, raising the need for an integrated framework that allows scholars to understand and study interactions of multiple "privacy layers".

This study sets out to examine individual online privacy behavior as an outcome of various aspects of life and society rooted in different levels of investigation. That is, it not only considers psychological influences on the individual level but includes economic, societal, cultural, and governmental aspects that may affect individuals' information privacy behavior. We define individual privacy behavior in terms of the decision-making process of whether and why individuals reveal personal information. For the research purpose, a systematic model derived from developmental psychology to the domain of information privacy is adopted, namely URIE BRONFENBRENNER's ecological multi-level model of human development,[8] thereby we introduce four interacting levels of information privacy. Hereby, the development of an overarching framework that subsumes the most important factors affecting individual privacy decisions uniquely complements prior literature. Summarizing interactions between layers, a new avenue for future research interested in systematically analyzing individual privacy behavior as a multi-level phenomenon is paved.

In the following, the basic assumptions of BRONFENBRENNER's model will be adapted in order to conceptualize information privacy around which individual behavior is modelled in the online world. Then, the characteristics of the four levels of information privacy will be outlined and their contribution to the explanation of individual privacy decisions discussed. Finally, the complex interactions that exist between the different layers and implications for theory and practice will be highlighted.

6 H. JEFF SMITH/TAMARA DINEV/HENG XU, Information Privacy Research: An Interdisciplinary Review, MIS Quarterly 2011, 989 ff., 990.

7 FRANCE BÉLANGER/ROBERT E. CROSSLER, Privacy in the Digital Age: A Review of Information Privacy Research in Information Systems, MIS Quarterly 2011, 1017 ff., 1039; SMITH/DINEV/XU (fn. 6).

8 URIE BRONFENBRENNER, Toward an experimental ecology of human development, American Psychologist 1977, 513 ff., 514.

Figure 1 depicts the model and gives an overview of how the text is structured.

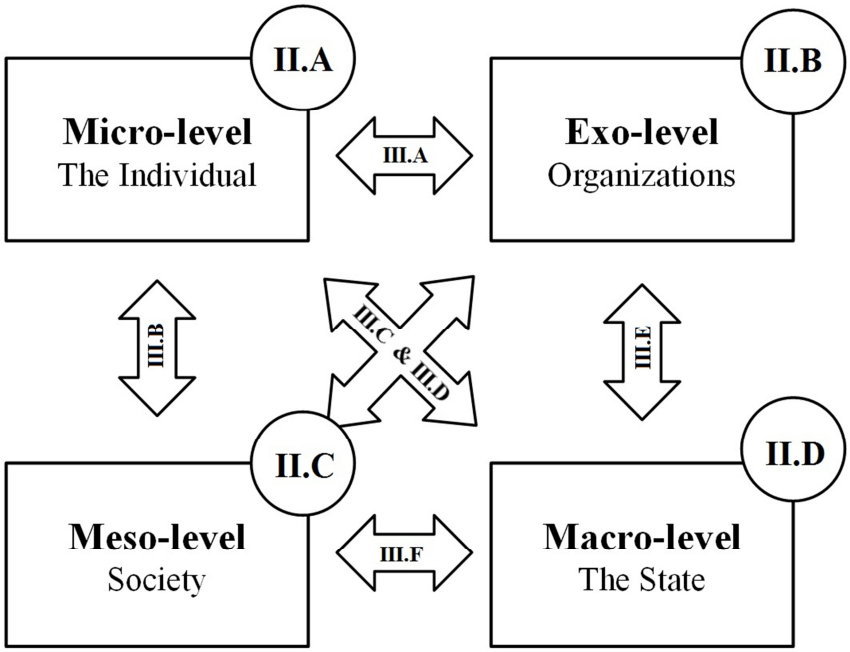


Figure 1: The Multi-Layered Privacy Interaction Framework (own depiction).

II. The Multi-Layered Privacy Framework

This article's integrative approach is based on BRONFENBRENNER'S ecological multi-level model of human development.[9] In this perspective, human development is described as a process in which an active, evolving person constantly interacts with his or her immediate environment.[10] That is, the individual is embedded in a constantly changing environment that consists of nested structures, or systems, such as families within communities within legal and cultural settings. While some layers may directly affect the individ-

9 BRONFENBRENNER (fn. 8).
10 BRONFENBRENNER (fn. 8), 513.

ual person and his or her development, systems may also interact with each other, resulting in an indirect impact on human development. Focusing on relations, BRONFENBRENNER regards interactions between individuals and their immediate environment as **microsystems**. In turn, he refers to social groups that do not have contact with the individual directly, such as neighbors or parental workplaces as **exo-systems**, while relations between social groups characterized by a large proximity to the individual are considered **meso-systems. Macro-systems**, finally, describe the structure that all other systems are embedded in, thus referring to laws, traditions and values of a whole society. Highlighting the complex and dynamic interactions of all systems with each other, BRONFENBRENNER's theory exhibits large ecological validity and has been successfully transferred to other areas of life and behavior, such as the functioning of (economic) organizations.[11]

Based on BRONFENBRENNER's assumption of a multi-level structure of an individual's environment, this article aims to describe individual decision-making in privacy-related situations as a reciprocal process of various layers interacting with and influencing each other. More precisely, it is assumed that individual privacy considerations are influenced by (1) individual cognitions and emotions at a micro-level, (2) stakeholders interested in personal data, such as economic organizations requesting information at an exo-level, (3) societal norms and values indirectly guiding individual decision-making at a meso-level, and (4) governmental decisions, regulations and laws at a macro-level. Fundamentally, this conceptualization follows BRONFENBRENNER's distinction between separate systems that constantly interact with individuals in a direct or indirect manner: Economic organizations, for example, are usually characterized by processes and decisions which are intransparent to the particular individual, while societal norms may directly shape individual behavior via societal groups, such as family members, or peers. Thus, the following layers relevant for an individual's privacy considerations can be distinguished: (1) individuals, (2) organizations, (3) society and (4) the government. This article suggests that privacy as a comprehensive phenomenon is rooted in all those layers and that privacy-related interactions between the different layers will affect individual decisions on information disclosure. In the following, rationales for these assumptions are provided by introducing characteristics of each layer and discussing their ongoing and reciprocal interactions.

11 JONAS CHRISTENSEN, Proposed Enhancement of Bronfenbrenner's Development Ecology Model, Education Inquiry 2010, 117 ff., 122.

A) Micro-Level: Individuals

The micro-level analyzes the interactions of an individual with his or her immediate environment, such as family members or peers. BRONFENBRENNER emphasizes the role of the settings in micro-systems, i.e., the role of the place, time and circumstances where interactions happen. Transferred to the context of privacy, this level comprises all interactions between a particular individual and the "data-requesting environment" in a particular setting. The micro-system embraces characteristics of the individual (e.g., concerns about privacy) and features of the data-requesting stakeholder, as well as the product or setting (e.g., design of the website that is asking for data). An individual deciding on whether to share a holiday picture with Facebook friends, for example, may predicate his or her decision on past privacy experiences, his general opinion on privacy and the inviting or non-inviting character of the Facebook website.

Against this background, the following chapter aims to highlight the dynamics of individual decision-making processes in the light of privacy-related cognitions and emotions. More precisely, the chapter aims to describe and explain (1) how individuals decide to disclose or not disclose data, (2) how characteristics of persons and situations influence this decision, and (3) why disclosing decisions sometimes contradicts individual preferences.

1. Individual's Privacy Calculus

Investigating the processes that underlie individual privacy-related decision-making in a certain situation, prior research was typically organized around two basic foundations: First, private information has generally been considered a commodity, i.e., a tradable good that individuals consciously barter in order to receive certain benefits.[12] In order to use the services provided by Facebook, for example, individuals have to accept the organization's privacy policy and authorize Facebook to use private data for various purposes. As such, private information is an "asset" or a "currency" bartered in return for benefits and value. Second, scholars have emphasized the rationality of decision-makers, stating that individuals anticipate privacy-related costs (or risks) as well as benefits arising from data provision, and from disclosing intentions and behavior as a result of this anticipatory, rational cognitive trade-off.[13] In

12 SMITH/DINEV/XU (fn. 6).

13 TAMARA DINEV/PAUL HART, An Extended Privacy Calculus Model for E-Commerce Transactions, Information Systems Research 2006, 61 ff., 64; CATHERINE L. ANDERSON/RITU AGARWAL, The Digitization of Healthcare: Boundary Risks,

the above example, therefore, potential Facebook users should carefully weigh risks and benefits connected to data provision before registering with the service or posting a holiday picture.

Emanating from these two foundations, empirical research on privacy-related decisions has widely adopted a "privacy calculus" perspective[14]: Individuals are expected to rationally anticipate and weigh privacy-related risks and benefits, and disclose their private information if the benefits outweigh the risks. Research organized around this perspective has successfully applied the privacy calculus framework in several domains, such as social media, mobile applications, or marketing. Moreover, numerous risk-enhancing and risk-mitigating factors exist: At a personal level, previous privacy experiences or personality traits, such as emotional stability, may enhance risk perceptions by enhancing individuals' concerns about privacy. Women tend to be more concerned about privacy, and Italians showed lower privacy concerns than U.S. citizens.[15] Furthermore, providing information that is more sensitive has repeatedly shown to constitute a risk-enhancing factor[16], while privacy notices or seals, generally, reduce individuals' concerns and perceptions of risk[17]. A professional look or an emotional appeal of the data-requesting website are also perceived as risk-mitigating.[18]

Emotion, and Consumer Willingness to Disclose Personal Health Information, Information Systems Research 2011, 469 ff., 475.

14 DINEV/HART (fn. 13); MARY J. CULNAN/PAMELA K. ARMSTRONG, Information Privacy Concerns, Procedural Fairness, and Impersonal Trust: An Empirical Investigation, Organization Science 1999, 104 ff., 106.

15 SMITH/DINEV/XU (fn. 6).

16 NARESH K. MALHOTRA/SUNG S. KIM/JAMES AGARWAL, Internet Users' Information Privacy Concerns (IUIPC): The Construct, the Scale, and a Causal Model, Information Systems Research 2004, 336 ff., 342; MOTHERSBAUGH/FOXX/BEATTY/WANG (fn. 2).

17 XIAORUI HU/GUOHUA WU/YUHONG WU/HAN ZHANG, The Effects of Web Assurance Seals on Consumers' Initial Trust in an Online Vendor: A Functional Perspective, Decision Support Systems 2010, 407 ff., 408; KAI-LUNG HUI/HOCK HAI TEO/SANG-YONG TOM LEE, The Value of Privacy Assurance: An Exploratory Field Experiment, MIS Quarterly 2007, 19 ff., 20.

18 LESLIE K. JOHN/ALESSANDRO ACQUISTI/GEORGE LOEWENSTEIN, Strangers on a Plane: Context-Dependent Willingness to Divulge Sensitive Information, The Journal of Consumer Research 2011, 858 ff., 859; FLAVIUS KEHR/DANIEL WENTZEL/PETER MAYER, Rethinking the Privacy Calculus: On the Role of Dispositional Factors and Affect, Proceedings of the 34th International Conference on Information Systems (ICIS) 2013, Milan, Italy.

2. Interfering with the Individual's Privacy Decision Making

2.1. Privacy-Paradox Dilemma

Empirical observations also point to inconsistencies in individual behavior when deciding on information disclosure. That is, studies repeatedly report that individuals disclose private information despite high self-assessed privacy-related worries and concerns. Denoted as the "privacy-paradox"[19], an increasing stream of literature discusses these deviations between attitudes and behaviors to be rooted in a distinction between dispositional tendencies and situational factors.[20] In this regard, situational cues are hypothesized to potentially override pre-existing attitudes, such as privacy concerns. Stated differently, factors unique to the data-requesting situation may be of higher importance than own attitudes when deciding on whether to provide information. Empirical research supports this explanation in showing that privacy concerns and behavioral outcomes are not consistent with each other if the data-requesting website offers specific benefits.[21] Moreover, recent research has shown that priming, salience shifting, or emotion influence privacy-related decisions[22], supporting the idea that individuals do not necessarily act in accordance with their attitudes, but are often persuaded to disclose personal information. Consequently, researchers have challenged the basic assumption of rationality in privacy-related decision-making, arguing privacy-related

19 PATRICIA A. NORBERG/DANIEL R. HORNE/DAVID A. HORNE, The Privacy Paradox: Personal Information Disclosure Intentions Versus Behaviors, Journal of Consumer Affairs 2007, 100 ff., 101.

20 HAN LI/RATHINDRA SARATHY/HENG XU, The Role of Affect and Cognition on Online Consumers' Decision to Disclose Personal Information to Unfamiliar Online Vendors, Decision Support Systems 2011, 434 ff., 435; KEHR/WENTZEL/MAYER (fn. 18).

21 NAVEEN FARAG AWAD/M. S. KRISHNAN, The Personalization Privacy Paradox: An Empirical Evaluation of Information Transparency and the Willingness to Be Profiled Online for Personalization, MIS Quarterly 2006, 13 ff., 14; HENG XU/XIN LUO/JOHN M. CARROLL/MARY B. ROSSON, The Personalization Privacy Paradox: An Exploratory Study of Decision Making Process for Location-Aware Marketing, Decision Support Systems 2011, 42 ff., 43.

22 BART P. KNIJNENBURG/ALFRED KOBSA/HONGXIA JIN, Counteracting the Negative Effect of Form Auto-Completion on the Privacy Calculus, Proceedings of the 34th International Conference on Information Systems (ICIS) 2013, Milan, Italy; JOHN/ACQUISTI/LOEWENSTEIN (fn. 18); JENS GROSSKLAGS/ALESSANDRO ACQUISTI, When 25 Cents Is Too Much: An Experiment on Willingness-to-Sell and Willingness-to-Protect Personal Information, Workshop on the Economics of Information Security 2007, New York, NY; KEHR/WENTZEL/MAYER (fn. 18).

decision-making to constitute an at least partially irrational process bounded by psychological limitations.[23]

2.2. Psychological Limitations and Irrational Privacy Decisions

Rational decision-making embraces careful consideration of all possible alternatives, and anticipation of their future consequences. In reality, however, individuals' access to this information is often limited due to bounded cognitive information processing capacity. Particularly, in a dynamic environment the probability of certain events in the future may be difficult to predict. Therefore, individuals often rely on cognitive "shortcuts", or cognitive heuristics, when taking decisions.[24]. For example, they rely on the most available rather than the most complete information, trust their feelings rather than rationality and show high needs for immediate gratification.[25]

In the context of information privacy, a small but increasing stream of literature explores the role of such heuristics in privacy-related decision-making. For example, ALESSANDRO ACQUISTI and others reveal that individuals tend to perceive benefits of data disclosure as more immediate, while privacy invasions are often invisible and only become apparent ex post.[26] As a result, the estimation of both the costs and benefits of information revelation may prove to be wrong. Accordingly, users may be "blinded" by ostensible benefits, such as personalization[27], and disclose their data without full rational processing. Similarly, individuals seem to generally be unaware of the public nature of the Internet[28], while at the same time raising their awareness on privacy-related issues, such as own privacy concerns, results in more conservative privacy decisions[29]. Moreover, prior work has shown that an in-

23 KEHR/WENTZEL/MAYER (fn. 18).

24 HERBERT A. SIMON, A Behavioral Model of Rational Choice, The Quarterly Journal of Economics 1955, 99 ff., 100.

25 MATTHEW RABIN/TED O'DONOGHUE, The Economics of Immediate Gratification, Journal of Behavioral Decision Making 2000, 233 ff., 234; TED O'DONOGHUE/MATTHEW RABIN, Choice and Procrastination, Quarterly Journal of Economics 2001, 121 ff., 122; HOWARD KUNREUTHER, Causes of Underinsurance against Natural Disasters, Geneva Papers on Risk and Insurance 1984, 206ff., 207.

26 ALESSANDRO ACQUISTI, Privacy in Electronic Commerce and the Economics of Immediate Gratification, Proceedings of the 5th ACM conference on Electronic commerce 2004, New York, USA.

27 AWAD/KRISHNAN (fn. 21).

28 SUSAN B. BARNES, A Privacy Paradox: Social Networking in the United States, First Monday 2006, retrieved from http://firstmonday.org/ojs/index.php/fm/article/viewArticle/1394/1312%2523 on 6 August 2014.

29 JOHN/ACQUISTI/LOEWENSTEIN (fn. 18).

creasing (as opposed to a random) sequence of information sensitivity results in less data provision[30], while more data was provided if communication with the computer was designed to be more intimate and reciprocal[31]. Emotional appeals, finally, seem to not only have the potential to shape individual risk and benefit perceptions in a privacy calculus, but to also override rational risk and benefit valuations.[32]

B) Exo-Level: Organizations

The exo-system encompasses areas of life where individuals are not actively engaged in, but are affected by processes and activities taking place within them.[33] In the context of privacy and the presented framework, organizations and companies in particular play the main role on the exo-level. This covers large Internet companies, such as Google, Facebook, Microsoft or Apple, mobile services providers – like Swisscom, Orange and Sunrise in Switzerland – but also an ecosystem of other players offering services and products related to privacy, therefore virtually every company or organization that has access to personal data. The companies forming the exo-system provide a myriad of online services from search to networking, from online shopping to cloud storage, from the so-called quantified self to behavioral feedback.

All these services rely to a varying degree on user data: they gather, store and process personal information to generate an eventually crucial output for the service. User data has become a valuable new currency. It does not only enable better customer relationship management, it also is a main resource for a variety of business models, from online networking sites to usage-based insurance. Accordingly, this chapter focuses on how organizations process, trade and expose user data.

Nowadays, electronic devices are well on the road to becoming ubiquitous. Sensors measure our moves; Facebook and Google almost know us better than our friends do and drones may soon accompany us everywhere and undertake the task of taking photos and making videos for us.[34] On the one hand, the implicitness with which new technologies are accepted encourages

30 ALESSANDRO ACQUISTI/LESLIE. K. JOHN/GEORGE. LOEWENSTEIN, The Impact of Relative Standards on the Propensity to Disclose, Journal of Marketing Research 2012, 160 ff., 161.

31 YOUNGME MOON, Intimate Exchange Using Computers to Elicit Self-Disclosure from Consumers, Journal of Consumer Research 2000, 323 ff., 324.

32 KEHR/WENTZEL/MAYER (fn. 18).

33 BRONFENBRENNER (fn. 8).

34 BBC News Technology, Video drone that flies itself, retrieved from www.bbc.com/news/technology-28178230 on 21 July 2014.

companies to keep developing them without paying great attention to consumer privacy. On the other hand, governments are not yet capable of keeping pace with fast development cycles and thus the potential for vast privacy breaches grows. In the following sections, we focus on two different organizational aspects of privacy. The first aspect refers to privacy issues arising for individuals in their role as service and product consumers and the second refers to privacy of institutional and corporate data.

1. Individual Privacy

(For profit) Internet organizations face different interests and stakeholders but to grow and sustain in the market they need to monetize their offerings. Since different Internet users have differing resources and various motivations to participate online[35] as well as vastly different privacy attitudes, organizations face a challenging task of offering the right service to the right user. Such customization has become possible and feasible with recent technological developments.[36] The type of personal information that is exposed and processed is changing – it is not only about facts (such as name, age, place of residence, etc.) but also about habits and behaviors. The influence that companies can potentially gain over individuals is huge. By tracking behavioral patterns such as eating, exercising, driving, sleeping, and virtually every second of one's life and also influencing them, companies get an exhaustive understanding of individuals.[37] Thus, they can offer value propositions based on personal user preferences. Targeted advertising on Facebook and personalized Google results are just the tip of the iceberg. Consumer data is not just needed for advertising but is usually sold to third parties for analytical purposes. Underneath the layer users get to see, i.e., targeted advertising and personalized search results, there exists a network of data brokers, ven-

35 CHRISTOPH LUTZ/CHRISTIAN PIETER HOFFMANN/MIRIAM MECKEL, Beyond just politics: A systematic literature review of online participation, First Monday 2014, 7, 1 ff., retrieved from http://firstmonday.org/ojs/index.php/fm/article/view/5260/4094 on 17 July 2014.

36 ZEYNEP TUFEKCI, Engineering the Public: Big Data, Surveillance and Computational Politics, First Monday 2014, 7, 1 ff., retrieved from http://firstmonday.org/ojs/index.php/fm/article/view/4901/4097 on 17 July 2014.

37 ROBINSON MEYER, Everything We Know About Facebook's Secret Mood Manipulation Experiment, The Atlantic 2014, retrieved from www.theatlantic.com/technology/archive/2014/06/every-thing-we-know-about-facebooks-secret-mood-manipulation-experiment/373648/ on 4 August 2014.

dors and sellers unknown to the general public.[38] This industry is rapidly growing.

In this light, profit-driven Internet companies tend to view user privacy (claims) as more of a nuisance than a value to protect. Emblematic sentences, such as Scott McNealy's, (CEO at Sun Microsystems) famous saying *"You have zero privacy, anyway, get over it"* document this attitude toward privacy as an outdated value. However, another emerging cluster of businesses is trying to include privacy-sensitive practices into their business models. "*We see today a growing number of tools meant to protect information by enabling users to code messages and emails, track and block third-party cookies and beacons (for example: Ghostery), browse the web anonymously (for example: Tor Project), get a rating of the website's level of "fairness" according to its privacy policy (for example: TosDR) and more*."[39]

2. Institutional Privacy

Not only private users but companies as well can become victims of privacy violations. Cyber risk refers to company data breaches that can lead to serious financial and reputational losses. As categorized by CHRISTIAN BIENER et al. cyber risk can be caused by actions of people, systems and technology failures, failed internal processes, and external events.[40] Data breaches are today's top concern for some companies. According to the ONLINE TRUST ALLIANCE 740 million data records were disclosed in 2013 and 89% of these incidents could have been prevented.[41]

Privacy breaches can have a great impact not only on the affected companies but also on their customers and in case of e.g. public utilities, on virtually everybody. One prominent example for a company data breach with huge consequences was the one made public in 2007 by TJX, one of the largest off-

38 CBS News, The Data Brokers: Selling your personal information, retrieved from www.cbsnews.com/news/the-data-brokers-selling-your-personal-information/ on 17 July 2014; Federal Trade Commission, May 2014, retrieved from www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf on 4 August 2014.

39 NILI STEINFELD, I Agree to the Terms and Conditions: (How) do Users Read Privacy Policies Online? An Eye-Tracking Experiment, ICA Annual Conference 2014, Seattle, USA, 5 ff., 6.

40 CHRISTIAN BIENER/MARTIN ELING/JAN WIRFS, Insurability of Cyber Risk, The Geneva Papers on Risk and Insurance 2014, 1 ff., 28.

41 ONLINE TRUST ALLIANCE, 2014 Data Protection and Breach Readiness Guide, retrieved from https://otalliance.org/system/files/files/resource/documents/2014otadatabreachguide4.pdf on 20 June 2014.

price apparel and home goods retailers in the US. Hackers stole customer payment information, which resulted in exposure of at least 45.7 million credit cards.[42] The data breach affected consumers whose identity was fraudulently used, banks and credit card companies who replaced payment cards, and a number of other businesses that experienced fraudulent transactions.

Even less sensitive information can do harm should it fall into the wrong hands. Large, aggregated and anonymized data sets still allow for a correct identification of individuals. For example, only four spatio-temporal points of reference with low resolution are enough to uniquely identify 95% of single cellphone users.[43] A data breach in the system of a telecommunication carrier can enable virtually anyone who has gained access to the information to extract individual human mobility traces. The arising constraints for individual privacy emphasize the urgency of minimizing cyber risks.

MARY J. CULNAN and CYNTHIA CLARK WILLIAMS suggest that companies should implement a culture of privacy and governance processes for privacy in order to avoid data breaches and the harm they cause to the involved parties.[44] They call for a corporate culture of moral responsibility that does not guarantee data privacy but at least makes it more likely that companies implement sound technical, structural, and procedural practices. Institutional privacy is gaining importance as more and more industries are heavily relying on information technologies to do their business. The TJX data breach is only one of numerous examples where organizations have failed to protect their data. As industry borders merge and networked businesses grow, knock-on effects from one failure can easily affect a serious part of the global economy and create a "Lehman moment" of the Internet, replicating the economic crisis from 2008 on a different level.

Individual behavior and willingness to provide personal data very much depends on the stand a company takes on privacy issues and how much people trust a company to handle personal data appropriately.

42 JOSEPH PEREIRA, How Credit Card Data Went Out the Wireless Door, The Wall Street Journal 2007, retrieved from http://online.wsj.com/news/articles/SB11782444 6226991797 on 22 June 2014.

43 YVES-ALEXANDRE DE MONTJOYE/CÉSAR A. HIDALGO/MICHEL VERLEYSEN/VINCENT D. BLONDEL, Unique in the Crowd: The privacy bounds of human mobility, Scientific Reports 2013, retrieved from http://dx.doi.org/10.1038/srep01376 on 19 July 2014.

44 MARY J. CULNAN/CYNTHIA CLARK WILLIAMS, How Ethics Can Enhance Organizational Privacy: Lessons from the ChoicePoint and TJX Data Breaches, MIS Quarterly 2009, 673 ff., 687.

C) Meso-Level: Society

Society describes a group of people who share a defined territory and a culture. Culture comprises norms, values, beliefs, practices, rituals, language, ideology, myths, and meanings given to symbols in a society.[45] Society and culture are closely interconnected as all societies have a culture and culture can only exist where there is a society. According to the culture dimension theory of GERT HOFSTEDE, which constitutes the most established conceptualization of culture, national culture is a "*collective programming of the mind which distinguishes the members of one group or category of people from another*".[46] Starting out from that thought, HOFSTEDE identified a taxonomy of five cultural value indices that apply to all cultures but vary in their magnitude: power distance, individualism, masculinity, uncertainty avoidance, and long-term orientation. Cultural values are characterized by strong beliefs that guide attitudes and behavior and that tend to endure even when other differences between countries are undermined by changes in economics, politics, technology, and other external effects.[47]

1. Culture's Role in Shaping Privacy Expectations

For the individual's valuation and interpretation of privacy, culture is of great importance. Culture shapes values and expectations and largely determines how people perceive data disclosure.[48] Even though information privacy is a universal matter, the specific concerns and responses to data requests depend on the individual's characteristics, including his or her culture. Considering the vast range of contextual roots, privacy has no single, simple definition but means different things to different people. The decision about whether and how much data to disclose is usually encompassed by the context, involving time, location, occupation, culture, or rationale.[49] Thus, the context either

45 CAROLINE LANCELOT MILTGEN/DOMINIQUE PEYRAT-GUILLARD, Cultural and generational influence on privacy concerns: a qualitative study in seven European countries, European Journal of Information Systems 2014, 103 ff., 107.

46 GEERT HOFSTEDE, Culture and Organizations: Software of the Mind, London 1991, 1 ff., 5.

47 GEERT HOFSTEDE, Culture's consequences: international differences in work-related Values, Beverly Hills (CA) 1980, 335 ff.

48 SANDRA J. MILBERG/SANDRA J. BURKE/H. JEFF SMITH/ERNEST A. KALLMAN, Values, personal information privacy, and regulatory approaches, Communications of the ACM 1995, 65 ff., 67.

49 GAURAV BANSAL/FATEMEH MIRIAM ZAHEDI/DAVID GEFEN, The moderating influence of privacy concerns on the efficacy of privacy assurance mechanisms for building

moderates or directly influences privacy relationships. The way information privacy is treated differs from culture to culture, and even citizens of countries in similar geographical areas display varying privacy concerns and online activities.[50]

With regard to the determinants of privacy concerns, cultural values and regulatory structures are the two macro-environmental factors most often examined. Hence, the relationship between culture and privacy concerns is of particular interest. The key cultural dimensions related to privacy are power distance, described by the degree to which a society tolerates higher or lower levels of inequality, and individualism versus collectivism, which defines "*the existence of strong cohesive groups and extended families that protect the individual in exchange for loyalty*".[51] Prior literature has identified the individualism/collectivism dimension as an explanatory factor for observed cross-cultural differences in privacy concerns.[52] However, the relationship remains contradictory: to date, there is no consensus about whether individualistic or collectivistic national cultures are more or less concerned about privacy. While some studies indicate that people from highly individualistic cultures hold fewer privacy concerns and are more comfortable disclosing high levels of data, other research suggests the opposite.[53]

2. A Cross-Cultural Comparison of Privacy Concerns

A cross-cultural comparison of the perceptions and concerns towards the privacy of personal information reveals that individuals in different countries exhibit different levels of privacy concerns. All societies do value privacy in some form, but the expression of privacy varies significantly across cultures.

Regarding privacy concerns in Switzerland, survey data indicates that about half of the Internet users are concerned about the use of their data for direct

trust: a multiple-context investigation, Proceedings of the 29th International Conference on Information Systems (ICIS) 2008, Paris, France.

50 STEVEN BELLMANN/ERIK J. JOHNSON/STEPHEN J. KOBRIN/GERALD LOHSE, International differences in information privacy concerns: a global survey of consumers, The Information Society 2004, 313 ff., 320.

51 ROWENA CULLEN, Culture, identity and information privacy in the age of digital government, Online Information Review 2009, 405 ff., 409.

52 CIGDEM KAGITCIBASI, Individualism and collectivism, in: John W. Berry/Marshall H. Segall/Cigdem Kagitcibasi (eds.), Handbook of Cross-Cultural Psychology: Social Behavior and Applications, Boston 1997, 1 ff., 3.

53 For an overview, see LANCELOT MILTGEN/PEYRAT-GUILLARD (fn. 45), 107.

marketing/junk ads, while the other half is not.[54] About 10% are very concerned and only about 3% are not concerned at all. This trend is in line with general findings in the rest of Europe. In the *Eurobarometer* survey, respondents were asked about their concerns when using social networking/sharing sites and online shopping sites.[55] For social networking/sharing sites, the use of information without the user's knowledge as the highest risk of disclosure is identified by the largest numbers of respondents of the then 27 EU member states (44%). When shopping online, the highest perceived risk is being a victim of fraud (43%). Although many citizens of the European Union are concerned about these risks, a country-by-country analysis shows different levels of privacy concerns: the highest scores for being concerned when information is used without the user's knowledge by social networking or sharing sites were found in Cyprus (72%), Romania (62%), Malta, and Ireland (both 61%). In contrast, only 31% and 35% of respondents are concerned about this risk in Portugal and in the UK. In the context of online shopping, being a victim of fraud is perceived as an exceptionally high risk in Bulgaria, where 67% of online shoppers evoke this concern. A high proportion of respondents also mentioned this risk in Cyprus (64%), Romania (60%) and Ireland (59%). On the other hand, the concern about being a victim of fraud is rather low in the UK (34%), Portugal, and Spain (both 35%).

In the Western Balkan the attitudes towards data protection and surveillance significantly differ by country.[56] While citizens from Croatia as well as from Bosnia and Herzegovina are mostly concerned about data protection, citizens from Serbia do not share this concern. With regard to surveillance, people from Macedonia hold positive attitudes, while in Serbia, the proportion of respondents concerned about being a surveillance target closely corresponds to the proportion of respondents opting for more surveillance.

With regard to the United States, data shows that 85% of Americans consider it very important to control access to their private data, and 72% express con-

54 CHRISTIAN HOFFMANN/CHRISTOPH LUTZ/MIRIAM MECKEL/GIULIA RANZINI, An Element of Surprise: The Impact of Serendipity on Online Trust, Annual Meeting of the Academy of Management 2013, Orlando, USA.

55 EUROPEAN COMMISSION, The Special Eurobarometer 359: Attitudes on Data Protection and Electronic Identity in the European Union, November-December 2010, TNS Opinion & Social, Brussels, retrieved from http://ec.europa.eu/public_opinion/archives/ebs/ ebs_359_en.pdf on 24 July 2014.

56 JELENA BUDAK/EDO RAJH/IVAN-DAMIR ANIC, Privacy Concern in Western Balkan Countries: Developing a Typology of Citizens, EIZ Working Papers 2014, retrieved from http://www.eizg.hr/Download.ashx?FileID=4b23edf2-f994-4dd3-9b57-7114747bfe14 on 24 July 2014.

cerns about firms tracking their online behavior.[57] An equal importance of privacy is found in Malaysia, where a vast majority (84%) is highly concerned. More than half of the respondents (56%) expressed concerns over their personal information being displayed in public, and another majority (64%) is highly concerned about the selling and trading of their personal information among companies.[58]

Overall, the results from different countries indicate that the privacy of personal information is a prime concern and that a lack of individual control over data evokes privacy anxiety. However, the findings also demonstrate that these universal issues emerge differently across countries and cultures, with emphases on particular foci. Such divergences reflect distinct cultural and political situations, historical experiences, and levels of economic development and thus lay different grounds for individual behavior.[59]

D) Macro-Level: State

The macro-level sets the normative structure within which society and markets and individuals interact. The main player in this field is the government acting as a regulator. In this role the government encompasses all norms, cultural aspects, opportunity structures, values, ideologies, conventions, hazards and legislations within a society.[60] In this context, these aspects are then included in (socially acceptable) written as well as unwritten rules. The macro-level combines the sum of relationships between the different systems into one normative context, in which certain values are regarded as crucial and

57 CONSUMERS-UNION, Consumer reports poll: Americans extremely concerned about internet privacy, 2008, retrieved from http://consumersunion.org/news/poll-consumers-concerned-about-internet-privacy on 24 July 2014; MARY MADDEN/SUSANNAH FOX/AARON SMITH/JESSICA VITAK, Digital Footprints: Online Identity Management and Search in the Age of Transparency, PEW Research Center Publications, retrieved from http://www.pewinternet.org/files/old-media/Files/Reports/2007/PIP_Digital_Footprints.pdf.pdf on 24 July 2014.

58 SUHAILA SAMSURI/ZURAINI ISMAIL, Personal Medical Information Management: The Information Privacy Culture of Asian Countries, Journal of Economics, Business and Management 2013, 329 ff., 330.

59 PHILIP N. HOWARD/NIMAH MAZAHERI, Telecommunications reform, Internet use and mobile phone adoption in the developing world, World Development 2009, 1159 ff., 1160.

60 URIE BRONFENBRENNER, Ecological models of human development, in: International Encyclopedia of Education, Vol. 3, 2. Aufl., Oxford 1994 reprinted in: Mary Gauvain/Michael Cole (Hrsg.), Readings on the development of children, 2. Aufl., New York 1993, 37 ff., 40.

others as less crucial for the functioning of the respective society and therefore, influencing an individual's privacy perception.

The government plays an important part in influencing the normative context of privacy issues within a given society. By means of legislation, it has the power to ensure stronger or weaker privacy rights and obligations for individuals, the private sector and itself. These rights are embedded in constitutions and legislation and determine the boundaries in which social interactions as well as economic transactions can flourish. Therefore, these regulations usually reflect social mores and culture of a society while shaping it at the same time. This is why information privacy regulations differ from country to country. Both individuals and companies are bound by this normative framework and therefore must comply with these regulations when it comes to decisions regarding privacy

1. Role of Governments

At the macro-level, the government has the role of a double-edged sword because its first obligation is to protect its citizens, thus acting as the safeguard of privacy. At the same time, regulators have to make sure that privacy legislation and data protection do not restrict economic growth and innovation.[61] Therefore, they have to balance conflicting interests at a general level, while also allowing case by case evaluations of privacy issues taking private and public interests into account. To add to the complexity of protecting privacy, a state itself has an interest in gathering information about its population in order to maintain internal and external security, public order and safety (in other the functioning of society as a whole). Furthermore, the state has to limit itself by guaranteeing individuals a certain level of data protection in order to reduce the existing power gap between them and the state.

For the government, the values of privacy are similar to the ones described in the chapter on the meso-level: for a democratic state to work, a citizen's right to feel free in all aspects of life, to act and to communicate without feeling like his or her every step is being watched by a third party, in particular the state, is crucial.[62] This sense of freedom is central to an individual's self-

61 A good example for the tension between innovation and regulatory regime is Germany that only allows the use of drones with the appropriate authorization. This discussion arose last year when Amazon announced that they plan to deploy drones for the delivery of their products, retrieved from www.spiegel.de/wirtschaft/unternehmen/amazon-jeff-bezos-will-mini-drohnen-einsetzen-a-936678.html on 5 August 2014.

62 SPIROS SIMITIS, Reviewing Privacy in an Information Society, 135 U. Pa. L. Rev. 707 1987, 707 ff., 734; EVGENY MOROZOV, The Real Privacy Problem, retrieved from

development which is a major aspect of privacy as a legal term.[63] The underlying value for data protection can therefore be deduced from an individual's sense of a private sphere that only he or she can decide upon and nobody else may interfere with. The government's obligation to protect this sphere goes hand in hand with the population's understanding of privacy.

2. Privacy as a Fundamental Right and Data Protection Norms

Privacy as a fundamental right plays an important role in one's self-development. Switzerland protects its citizens' data in the constitution with the right to informational self-determination (Art. 13 para. 2 Swiss Federal Constitution (BV)) giving it the same significance as for example the freedom of expression (Art. 16 BV). The right to informational self-determination entitles individuals to decide to whom, when and where their personal data is disclosed. In Europe, a person's right to informational self-determination is understood as a human right. According to Art. 8 of the European Convention of Human Rights (ECHR) citizens are entitled to the protection of their private and family life from the government which includes their homes and correspondence. This basic human right can only be restricted by legislation in case public interests such as national security, public safety or the economic well-being of a country are at stake (Art. 8 para. 2 ECHR). The same rules are stated in Art. 8 of the Charter of Fundamental Rights of the EU (CFREU) and as such apply to the European Union as a whole. This legal mechanism of government interference is central for the functioning of a democratic state. However, the interference of a government with its citizens' privacy is limited and bound by the proportionality principle when it comes to weighing said public interests against an individual's data protection rights. This fundamental rights approach is peculiar to the European understanding of privacy. U.S. legislation offers a much narrower understanding of data protection at a constitutional level.[64]

Moreover, common data protection principles were established at the same time as the first data protection acts were enacted. These fundamental principles are stated in the Council of Europe's Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (binding)

http://www.technologyreview.com/featuredstory/520426/the-real-privacy-problem/ on 5 August 2014.

63 ULRICH HÄFELIN/WALTER HALLER/HELEN KELLER, Schweizerisches Bundesstaatsrecht, eighth ed., Zurich 2012, 125; JÖRG PAUL MÜLLER/MARKUS SCHEFER, Grundrechte in der Schweiz, Im Rahmen der Bundesverfassung, der EMRK und der UNO-Pakte, fourth ed., Berne 2008, 138.

64 See chapter III. F).

and have also been internationally recognized in the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (soft law). These internationally recognized principles lay down the ground on which the data protection legislation in the EU and Switzerland is based thus, making these principles enforceable in these countries' jurisdictions. Among others, these norms set limits to the collection and use of personal data (Collection Limitation Principle & Use Limitation Principle), and establish the following guidelines: collected data must be relevant for the envisaged data processes (Data Quality Principle), the purpose for which the personal data is collected must be specified prior to the collection (Purpose Specification Principle), and data must be secured against unauthorized third parties (Security Safeguards Principle).[65] Existing national data protection rights – be it hard or soft law – are not (easily) enforceable across borders due to the territoriality principle, even if they are statutory in the country the breach occurred.

III. Interactions between the Layers

Most research exploring irrationality in information privacy has focused on situational rather than personal factors, suggesting relations in the micro-system to be more strongly driven by situation rather than person. As such, creating fair and non-intrusive situations may constitute a key issue to ensure individuals take decisions that match their beliefs and preferences. Consequently, the significance and responsibility of entities and actions on the meso-, exo- and macro-levels increase. Stated differently, if individual privacy decisions are heavily biased by situational cues, then entities capable to create and change such cues become irreplaceable – for example, organizations that provide just and transparent privacy policies, societies that develop sensible and privacy-friendly social norms, or governments that find laws and regulations that protect private life and behavior.

The following sections therefore highlight the importance of the interactions among the different levels (for an overview see figure 1). An example for each interaction points to important aspects and depicts the practical relevance of the interaction.

65 OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data 1980 and its updated version 2013 (Principles are unchanged).

A) Individual – Organizations

Many individuals are regularly confronted with the main proponents of the exo-system, i.e., Internet companies, although they do not form part of them and shape them in active ways. In that sense and following the definition of the exo-system outlined above, most individuals are not in direct contact with exo-system actors (e.g., Facebook and Google as companies) only their services. At the same time, they are affected by the exo-system and its decisions. Individuals can choose or are forced to adopt products and services developed by the exo-system, which, in turn, diffuses their offers to as many individuals as possible. Adopting a product or service, however, undoubtedly connects to sharing information, as RUST et al. emphasize: *"(…) it may be quite impossible for customers to transact business on the Internet without revealing information about themselves that they may be unwilling to share*".[66] In that sense, individuals have no choice but to provide personal data in order to use a service.

The most obvious privacy intersection between the individual and the organization in the Internet context is the privacy policy. On the one hand, companies need to specify how they use their customers' or users' data. Users, on the other hand, by agreeing to the privacy policy, enter a contractual agreement with the organization that it can use their data for the intended purposes. This principle has been termed "notice and consent"[67] and seems a fair approach at first sight. However, notice and consent suffers from a serious issue, namely that many users are not able to understand privacy policies. Accordingly, studies show that many users do not read privacy policies[68] and are therefore not fully aware of their privacy rights and duties on the Internet with regards to organizations. ALEECIA M. MCDONALD and LORRIE F. CRANOR

66 ROLAND T. RUST/P. K. KANNAN/NA PENG, The Customer Economics of Internet Privacy, Journal of the Academy of Marketing Science 2002, 455 ff., 455.

67 FRED H. CATE/VIKTOR MAYER-SCHÖNBERGER, Notice and Consent in A World of Big Data, International Data Privacy Law 2013, 67 ff., 67.

68 JAY P. KESAN/CAROL M. HAYES/MASOODA BASHIR, Consumer Privacy Choices, Informed Consent, and Baseline Protections to Facilitate Market Transactions in the Cloud, Illinois Program in Law, Behavior and Social Science 2012, 11 ff.; JULIO ANGULO/SIMONE FISCHER-HÜBNER/ERIK WÄSTLUND/TOBIAS PULLS, Towards Usable Privacy Policy Display & Management - The PrimeLife Approach, Proceedings of the Fifth International Symposium on Human Aspects of Information Security & Assurance (HAISA) 2011, 108 ff.; JANICE Y. TSAI/SERGE EGELMAN/LORRIE CRANOR/ALESSANDRO ACQUISTI, The Effect of Online Privacy Information on Purchasing Behavior: An Experimental Study, Information Systems Research 2011, 254 ff.; DAVID B. MEINERT/DANKE K. PETERS/JOHN R. CRISWELL/MARTIN D. CROSSLAND, Privacy policy statements and consumer willingness to provide personal information, Journal of electronic commerce in organizations 2006, 1 ff.

calculated that "*if all American internet users would read every privacy policy they signed, the American nation would spend about 54 Billion hours a year reading these statements, an average of 40 minutes a day for each citizen*".[69] Thus, the relationship between organizations and (most) individuals is not one on a level playing field, since organizations have substantially more expertise and resources in terms of privacy.

Privacy advocates have therefore called for an empowerment of the user that goes beyond privacy policies and uses "privacy by design"[70] or approaches the topic in a more nuanced way via "contextual privacy"[71]. The former framework avers that privacy should be embedded into technological solutions and new applications should be designed in a privacy protecting mode from the beginning on. User friendly default settings, which respect privacy, are a first step in this direction. An exemplary application for privacy by design is Open PDS.[72] The contextual privacy approach argues that Internet companies should ask users for permission to use their data depending on the privacy norms at play, i.e., on the context, instead of on a "catch-it-all" basis. Thus, it brings context back into play.

As we saw above (cf. chapter II. A) 2.1), individuals' privacy decisions are often situational, while their attitudes are more permanent. Thus, by setting the "right" incentives and by offering contextually useful value propositions, organizations can leverage users' willingness to disclose and turn them into valuable datasets. This goes well beyond mere privacy policies and includes the layer of technological affordances, where specific values are embedded and encoded.[73] Such encoded principles strongly define users' privacy experience. The interactions between the individual and the organizational sphere – and especially the aspect of affordances – will be outlined with a current and well-known example: Facebook.

69 ALEECIA M. MCDONALD/LORRIE F. CRANOR. The Cost of Reading Privacy Policies, I/S: A Journal of Law and Policy for the Information Society 2008, 540 ff.

70 ANN CAVOUKIAN. Privacy by Design – The 7 Foundational Principles, Information and Privacy Commisioner, Ontario, Canada 2009, 1 ff., retrieved from https://www.iab.org/wp-content/IAB-uploads/2011/03/fred_carter.pdf. on 5 August 2014; STEINFELD (fn. 39).

71 HELEN NISSENBAUM, A Contextual Approach to Privacy Online, Daedalus 2011, 32 ff., 32.

72 Open PDS, retrieved from http://openpds.media.mit.edu/ on 5 August 2014.

73 DANAH BOYD, Autistic Social Software, Suepernova Conference 2004, retrieved from http://www.danah.org/papers/Supernova2004.html on 5 August 2014.

Facebook

Facebook's privacy approach becomes apparent in its privacy policy that specifies the company's use of users' personal data.[74] After global criticism Facebook gradually made its privacy policy increasingly user-friendly and approachable.[75] More subtly and less visibly, though, Facebook handles privacy through its technological affordances.[76] The way its interfaces are programmed and designed shapes users' privacy experiences.[77] Thus, while early Facebook had a "public by default" approach, today its privacy options are much more nuanced and users increasingly choose the private mode.[78]

Current research on Facebook privacy indicates that users are becoming more aware of the social privacy risks at play but not so much the institutional ones.[79] Accordingly, there has been a shift in Facebook users' privacy settings from "public" to – more and more – "private".[80] Therefore, users increasingly understand the potential privacy risks in their immediate surroundings and are afraid of too much access by certain persons. However, ALISON L. YOUNG and ANABEL QUAN-HAASE's study also shows that institutional privacy concerns are much less pronounced than social privacy concerns.[81] Hence, most users are not concerned about institutions – such as secret services or the state – or companies invading their privacy on the Internet. While social privacy risks – such as stalking, bullying or reputational damage – are very present in users' everyday life, the institutional risks are perceived as

74 FACEBOOK Privacy Policy, retrieved from https://www.facebook.com/about/privacy/ on 5 August 2014.

75 VAN JENSEN, As Chief Privacy Officer at Facebook, Richter has Friends (and Critics) in High Places, UPenn Law 2011, retrieved from https://www.law.upenn.edu/live/news/1952-as-chief-privacy-officer-at-facebook-richter-has#.U6iNcfl_uSo on 5 August 2014.

76 DANAH BOYD, Social Network Sites As Networked Publics: Affordances, Dynamics and Implications, in: Zizi Papacharassi (ed.), A Networked Self: Identity, community, and culture on social network sites, New York 2010, 39 ff.

77 FRED STUTZMAN/JACOB KRAMER-DUFFIELD, Friends Only: Examining a Privacy-Enhancing Behavior in Facebook, Proceedings of the 28th CHI Conference 2010, Atlanta (GE), USA, retrieved from http://dl.acm.org/citation.cfm?id=1753559 on 5 August 2014.

78 DANAH BOYD/ESZTER HARGITTAI, Facebook Privacy Settings: Who Cares, First Monday 2010, 8, 1 ff., retrieved from http://firstmonday.org/ojs/index.php/fm/article/viewArticle/3086 on 7 August 2014.

79 ALISON L. YOUNG /ANABEL QUAN-HAASE, Privacy protection strategies on Facebook: The Internet privacy paradox revisited, Information, Communication & Society 2013, 479 ff.

80 Public in this context means visible to everyone, while private means only visible to friends or a subset of friends. BOYD/HARGITTAI (fn. 78).

81 YOUNG/ QUAN-HAASE, (fn. 79).

much more remote and abstract. This phenomenon has been viewed through a sociological lens which depicts that the abstract risks are attributed to the society-level, whereas the more immediate – social risks occur at the community-level.[82] Thus, companies like Facebook can leverage this aspect and – via privacy settings, friend lists and groups – provide instruments for a seemingly controlled (and private) user experience, while concealing the institutional aspects at the same time. Yet, Facebook is increasingly reacting to criticism and is beginning to view privacy as part of its business model.[83]

B) Individual – Society

With regard to the meso-level, individual decision-making is not only caused by psychological considerations but also by aspects of socialization into prevalent social norms. Social norms are affected mostly by culture and are not necessarily rational by nature. Culture shapes values and expectations and largely determines how people perceive data disclosure.[84] Even though information privacy is a universal matter, the specific concerns and responses to data requests depend on the individual's characteristics, including his or her culture. The decision about whether and how much data to disclose is usually encompassed by the context, involving time, location, occupation, culture, or rationale.[85] Therefore, the cultural context either moderates or directly influences privacy relationships.

The way information privacy is treated differs from culture to culture, and even citizens of countries in similar geographical areas display varying privacy concerns and online activities.[86]

Besides the spatial dimension, the temporal dimension also plays a key role in the interaction between an individual and society. The notions of privacy change during an individual's life (age and generation effects) and over long(er) timespans. On the one hand, current notions of privacy are shifting.

82 CHRISTOPH LUTZ/PEPE STRATHOFF, Privacy Concerns and Online Behavior – Not so Paradoxical After All: Viewing the Privacy Paradox through Different Theoretical Lenses, in: Sandra Brändli/Roman Schister/Aurelia Tamò (eds.), Multinationale Unternehmen und Institutionen im Wandel – Herausforderungen für Wirtschaft, Recht und Gesellschaft, 8. Schriftenreihe der Assistierenden der Universität St.Gallen, St.Gallen 2013, 81 ff.

83 STEFAN SCHULZ, Sogar Facebook entdeckt noch Neuland, FAZ Blog 2014, retrieved from http://blogs.faz.net/digitaltwin/2014/07/28/facebooks-will-jetzt-privatsphaere-765/ on 5 August 2014.

84 MILBERG/ BURKE/SMITH/ KALLMAN (fn. 48), 67.

85 BANSAL/ ZAHEDI/ GEFEN (fn. 49).

86 BELLMANN/JOHNSON/KOBRIN/LOHSE (fn. 50), 320.

Thus, what counted as private 50 years ago is not necessarily private today. On the other hand, notions of privacy differ by an individual's age. These effects are affiliated to the individual's socialization. Although media representation portrays young users' as devoid of any sense of privacy[87], academic research has shown that most adolescents are well able to balance their needs for privacy with their desire for expression.[88] DANAH BOYD concluded from her study that the teens she met "*genuinely care about their privacy, but how they understand and enact it may not immediately resonate or appear logical to adults. […]Teens are not particularly concerned about organizational actors; rather, they wish to avoid paternalistic adults who use safety and protection as an excuse to monitor their everyday sociality*".[89]

Differences in Twitter Usage

The microblogging/social network service Twitter is used throughout the world. Yet, there exist considerable differences in the share of Internet users that are active on Twitter and on the functions that Twitter is used for. In the US, nearly 20% of internet users use Twitter, whereas that share is only 7% for Germany and 11% for Switzerland.[90] This might be partly explained by the unsuitability of the German language to condense complex information into 140-character Tweets, by Twitter's relatively weak structures in Germany or by the lack of opinion leaders in Germany and Switzerland that actively use and promote Twitter.

However, cultural differences and attitudes towards privacy seem to play a major role in accounting for the observed differences in Twitter usage. As a hybrid between a social network site and a microblogging tool, all communication on Twitter is inherently public. Tweets can be found with search engines and can be retweeted even without a follower relationship. This makes Twitter more susceptible for privacy concerns than e.g. Facebook, where users can – at least at the surface – control, who can access their information and communication. People in German-speaking countries tend to have more concerns about privacy and see their expression of opinion on political respectively societal issues as a private affair. This might explain, why Twitter

87 DANAH BOYD, It's Complicated: The Social Lives of Networked Teens 2014, New Haven, CT, Yale Unviersity Press, 1 ff., 55.

88 BOYD (fn. 87).

89 BOYD (fn. 87), 56.

90 STEFAN DOERNER, Fünf Gründe, warum Deutschland nicht twittert, The Wall Street Journal Online 2014, http://blogs.wsj.de/wsj-tech/2014/06/24/twitter-deutschland/ on 20 October 2014; CHRISTIAN MESSIKOMMER, Die Schweiz in Tweets, Tages-Anzeiger Online 2014, retrieved from http://www.tagesanzeiger.ch/digital/social-media/Die-Schweiz-in-Tweets/story/10677006 on 20 October 2014.

in Germany and Switzerland is rather used by people in their professional roles, who want to keep up to date with news from opinion leaders and experts and promote their own work. Twitter is, thus, a good example of how societal norms and cultural differences shape the individual's online behavior.

C) Individual – State

When providing data to governmental institutions individuals often have higher concerns and lower levels of trust compared to sharing such information with other parties such as NGOs or for-profit organizations (cf. chapter II. B) 2).[91] Indeed, the relation between the state and citizens in terms of privacy is rather imbalanced, due to the fact that the state possesses a monopoly of power, which to a certain extent has been mitigated with freedom of information legislation such as the Freedom of Information Act in the US or Switzerland's Federal Act on Freedom of Information in the Administration (BGÖ). These allow individuals' insight to specific government held documents upon request (5 U.S.C. § 552 (b) (6) & (7) (C); Art. 3 BGÖ). The government can deny or restrict access to information under certain circumstances for example if the request compromises the decision-making process of an authority or the domestic and international security of Switzerland (Art. 7 BGÖ). Some institutions of the state such as the police and secret services can – under certain circumstances – monitor their citizens and invade their privacy by way of legislation and for reasons of public interests (cf. chapter II D) 2). This includes methods like wiretapping but more recently also online tracking and spying.

On the other hand, the state regulates why and how privacy infringements are punished. Its legislation touches upon topics as diverse as stalking and cyberbullying or harassment, but can also extend to fraud prevention or civil rights protection. As a response to an increasing number of e-commerce transaction frauds, for example, a recent German law amendment obliges vendors to explicitly indicate transaction costs by labeling order buttons appropriately (§ 312j *Bürgerliches Gesetzbuch* (BGB)). Given the unawareness of individuals on the public nature of the Internet,[92] similar policies could help to raise individual awareness on privacy issues.

Although the state possesses more power compared to individuals, citizens have certain means to enforce their privacy rights. One such way is via law-

91 CATHERINE L. ANDERSON/RITU AGARWAL, The Digitization of Healthcare: Boundary Risks, Emotion, and Consumer Willingness to Disclose Personal Health Information, Information Systems Research 2011, 469 ff.

92 BARNES (fn. 28).

suits. Citizens can go to court and try to reclaim their privacy from other citizens, organizations or the state itself. In Switzerland, petitions and referendums are a way of directly influencing the country's legislation. However, so far no initiative or referendum on information privacy has come to the ballot box since the enactment of the Federal Data Protection Act (*Datenschutzgesetz*) in 1993. Finally, the official way of influencing politics via voting can also change the state's privacy agenda, as the rise of the Pirate Parties – which give online privacy issues a central place in their party programs – in several European countries and cities has shown.[93]

Swiss "Nachrichtendienstgesetz" (NDG)

Switzerland has relatively strict privacy laws compared to other countries outside of the EU, such as the U.S. (cf. chapter D)) and citizens are well protected from state surveillance. Nevertheless, new developments might challenge this situation. The Swiss *Nachrichtendienst des Bundes* (National Security Agency, NDB) is one of the bodies to ensure national security in Switzerland and its main task is to collect, analyze, evaluate and forward information to the responsible bodies in order to help secure Switzerland as a nation while still respecting individual's privacy.[94] The reform of the Swiss Security and Intelligence Act, *Nachrichtendienstgesetz* (E-NDG), which was debated in the security commission of the Swiss Parliament in August this year, challenges certain aspects of citizens' privacy rights and as of November 2014 will be in force.[95] It allows the Swiss secret service to preventively monitor

93 GISSUR Ó. ERLINGSSON/MIKAEL PERSSON, The Swedish Pirate Party and the 2009 European Parliament Election: Protest or Issue Voting?, Social Science Computer Review 2011, 121 ff.

94 Botschaft zum Nachrichtendienst vom 19. Februar 2014 (Botschaft zum Nachrichtendienstgesetz), 5, retrieved from http://www.news.admin.ch/NSBSubscriber/message/attachments/33837.pdf on 5 August 2014.

95 MARKUS HÄFLIGER, Neues Ungemach für Ueli Maurer, NZZ Online 2014, retrieved from http://www.nzz.ch/schweiz/neues-ungemach-fuer-ueli-maurer-1.18321851 on 5 August 2014; see further: Rainer J. Schweizer, Ein neues Staatsschutzgesetz?, Sicherheit & Recht, 3/2013, pp. 123-135; The Swiss government has accepted the revised NDG, see press release: "Bundesrat setzt das revidierte Bundesgesetz über die Zuständigkeiten im Bereich des zivilen Nachrichtendienstes in Kraft", retrieved from http://www.vbs.admin.ch/internet/vbs/de/home/documentation/news/news_detail.54752.nsb.html on 10 October 2014; PHILIPP LOSER, Kritik an Spionagegesetz verstummt, Tages-Anzeiger 2014, retrieved from http://www.tagesanzeiger.newsnet.ch/schweiz/standard/Kritik-am-Spionagegesetz-verstummt/story/13603082 on 22 October 2014.

suspicious citizens by using wiretaps, tracking mobile phones, hacking computers via Trojans and other privacy invading methods.[96] Furthermore, this can enable the NDB to collect more information – personal data – than ever before. However, in order to conduct such far-reaching surveillance the NDB will have to first consult the Federal Council's (*Bundesrat*) Security Commission and then seek prior authorization from the Swiss Federal Administrative Court and the Federal Department of Defence, Civil Protection and Education (VBS) (Art. 25 ff. E-NDG).[97] Moreover, the list of surveillance methods that do not require prior authorization such as public information sources will be expanded so that full use of new technologies can be guaranteed to secure Switzerland (Art. 13 ff. E-NDG).

The Swiss government says this reform is necessary in order to ensure national security at the same level as other countries like the U.S. do.[98] Foreign intelligence agencies such as the NSA are a further reason why the Swiss government wants to expand its national security methods. The government argues that in order to ensure higher privacy protection against agencies like the NSA, technology has to increasingly be deployed in Switzerland and therefore greater invasions in a person's privacy have to be allowed.[99] The new measures in the E-NDG received a lot of criticism from the public, privacy advocates and even members of Parliament who initially supported the reform. This is because the privacy of individuals' suffers from less protection now that the reform has been revised and enacted.[100] Thus, individuals might be stifled in the way they conduct their everyday life ("chilling-effect") due to greater privacy concerns and the fear of more surveillance.

The NDG example shows the substantial power imbalance between citizens and the state in terms of online privacy but also presents the government's role of a double-edged sword.[101] On the one hand, national security requires far reaching but proportional privacy invasions. On the other hand, these measures must protect citizen's privacy as far as possible at the same time.

96 Botschaft zum Nachrichtendienstgesetz (fn. 94), 9.

97 Botschaft zum Nachrichtendienstgesetz (fn. 94)

98 Botschaft zum Nachrichtendienstgesetz (fn. 94), 11; For further comments see: http://grundrechte.ch/CMS//botschaft-zum-nachrichtendienstgesetz.html retrieved on 5 August 2014.

99 Botschaft zum Nachrichtendienst (fn. 94), 11 f.

100 MARKUS HÄFLIGER, Schweizer Geheimdienst soll aufrüsten, NZZ Online 2013, retrieved from http://www.nzz.ch/aktuell/schweiz/neuer-anlauf-fuer-den-lauschangriff-1.18043256 am 5 August 2014; JAN FLÜCKIGER, Kritik am neuen Nachrichtengesetz, NZZ Online 2014, retrieved from http://www.nzz.ch/aktuell/schweiz/kritik-am-neuen-nachrichtendienstgesetz-1.18292791 on 5 August 2014.

101 Botschaft zum Nachrichtendienst (fn. 94), 10.

D) Organizations – Society

Organizations are shaped by society and its values. They "soak up" specific norms and reproduce them as part of their organizational and corporate identity.[102] However, the exo-system is not only shaped by society and its (privacy) norms and values, it also actively shapes them as noted by PETER F. DRUCKER.[103] Facebook, Google, Apple and other examples show that organizations do not exist in a value-free space but are themselves highly normative and "ideological" constructs, bringing about shifts in values and norms and creating trends. Facebook, for example has been accused of creating a narcissistic, shallow and individualistic culture, where impressions count more than real feelings[104] and privacy is eroded.[105] The company's missionary zeal of making individuals more sharing and connected, its very narrow and restricted employee background,[106] mixed with its history, and its strong dependence on user data contribute to a marginalization or exclusion of privacy-related issues.

Many major tech companies promote themselves as advocates of sharing, transparency and openness and these values play a very strong role not only in the rhetoric of the companies[107] but also in their daily practices – and accordingly in their products and services.[108] Such an ideology has been criti-

102 STUART ALBERT/DAVID A. WHETTEN, Organizational Identity, in: Mary Jo Hatch/Majken Schultz (eds.), Organizational Identity – A reader, Oxford 2006, 89 ff.; MARY JO HATCH/MAJKEN SCHULTZ, The Dynamics of Organizational Identity, in: Mary Jo Hatch/Majken Schultz (eds.), Organizational Identity – A reader, Oxford 2006, 377 ff.

103 PETER F. DRUCKER, The New Society of Organizations, Harvard Business Review 1992, 95 ff.

104 One of the most prominent proponents of this view is Sherry Turkle. SHERRY TURKLE, Alone Together: Why We Expect More From Technology and Less From Each Other, New York 2011.

105 JONATHAN SHAW, The erosion of privacy in the Internet era, Harvard Magazine 2009, retrieved from http://harvardmagazine.com/2009/09/privacy-erosion-in-internet-era on 5 August 2014.

106 MAXINE WILLIAMS, Building a More Diverse Facebook, Facebook newsroom 2014, retrieved from http://newsroom.fb.com/news/2014/06/building-a-more-diverse-facebook/ on 5 August 2014; MATTHEW MULLENWEG, Mitch Kapoor vs. Mark Zuckerberg, retrieved from http://ma.tt/2007/03/kapor-vs-zuckerberg/ on 5 August 2014.

107 Some quotes by Mark Zuckerberg exemplify this: «By giving people the power to share, we're making the world more transparent.» and «The thing that we're trying to do at Facebook is just to help people connect and communicate more efficiently.»

108 LIAM MITCHELL, Life on automatic: Facebook's archival subject, First Monday 2014, 2, 1 ff., retrieved from http://firstmonday.org/ojs/index.php/fm/article/view/4825 on 5 August 2014.

cally termed as "social missionaries",[109] "solutionism",[110] or "Californian Ideology".[111] All these notions imply a technological determinism and naive belief in the power of technology to solve social problems.[112] Google's, Apple's and other companies' mission of connecting people and nudging them to be more open and sharing ultimately results in an "archival subject" – a subject that has a passion to constantly quantify and archive his/her life. "*Zuckerberg understands this captured, transparent, happily sharing Facebook user to be an inevitable product of history. For instance, applying Moore's Law to sharing, he claims that 'ten years from now people will be sharing about a thousand times as many things'.*"[113] Such a transparent society lays open its – unique and "correct" – identity[114] and expresses itself freely in its social environment. But in expression also lie risks of exposure and privacy threats. One area where such threats are especially salient is cloud computing, as the following example depicts.

Dropbox & Wuala

A good example for the interaction between organizations and society are the two cloud services "Dropbox"[115] and "Wuala"[116]. Essentially, both services offer the same product, but Dropbox is a Silicon Valley company and Wuala a Swiss company, founded at the Swiss Federal Institute of Technology (ETH). Dropbox underlines sharing and ease of use as core components of its service but not user privacy and security. Wuala, by contrast, focuses much more on encryption, security and privacy – using the Swiss colors and Swissness (safety) prominently in its corporate identity. Dropbox has repeatedly been accused of lax security settings, undermining the privacy of its users. By

109 MITCHELL (fn. 108).

110 EVGENY MOROZOV, To Save Everything Click Here, New York 2013.

111 RICHARD BARBROOK/ANDY CAMERON, The Californian ideology, Science as Culture 1996, 42 ff.; KATE RAYNES-GOLDIE, Privacy in the age of Facebook: Discourse, architecture, consequences," unpublished doctoral thesis, Department of Internet Studies, Curtin University (January), 2012; KATE RAYNES-GOLDIE, The philosophy of Facebook (or, the real reason Facebook doesn't care about privacy), k4t3.org 2010, 2 December.

112 In fact, "solving problems" is a pertinent term used by tech companies to describe their approach of developing new applications.

113 MITCHELL (fn. 108).

114 One of Mark Zuckerberg's most famous quotes illustrates this: "You have one identity. Having two identities for yourself is an example of a lack of integrity." (quoted from MITCHELL, (fn. 108), 11.

115 WIKIPEDIA, Dropbox, retrieved from http://en.wikipedia.org/wiki/Dropbox_(service) on 5 August 2014.

116 WIKIPEDIA, Wuala, retrieved from http://en.wikipedia.org/wiki/Wuala on 5 August 2014.

contrast, Wuala – and the Swiss industry for data and privacy protection in general[117] – make clever use of users' privacy considerations and desires. It puts security and encryption at the center of its approach. Despite the differences in corporate image and norms and values at stake, a *Fraunhofer* study shows that both companies are in fact quite similar in their core performance categories.[118] Thus, Wuala reflects the stricter privacy laws and understanding of Switzerland whereas Dropbox as a US company is based on different values.

E) Organizations – State

The interactions between organizations and the state are manifold. By regulating privacy and setting guidelines and rules, the state directly influences organizations' offerings. Thus, the exo-system is embedded in a pre-existing but constantly evolving environment of rules, laws, and regulations. However, compared to the state, organizations are less inert, quicker at innovating and adapting. They can venture into unknown territory, where no or little legislation and regulation exists.[119] In balancing the normative claims of the state with a myriad of individual needs on the side of the consumer, organizations face a challenging task. Privacy is thus constantly negotiated between corporate interests – also in terms of organizational privacy – individual needs and desires, and regulatory agreements as well as cultural and societal norms. This complexity becomes especially salient in the case of multinational companies, where it is not always clear which privacy regulations (should) apply.[120]

117 LAURA SECORUN PALET, From Banking Paradise to Data Hub, OZY 2014, retrieved from http://www.ozy.com/fast-forward/swiss-data-banks/32627.article#.U7-4XauwPdU.twitter on 5 August 2014.

118 HENNING STEIER, Man kann sich das Hochladen sparen, Neue Zürcher Zeitung 2014, retrieved from http://www.nzz.ch/aktuell/digital/fraunhofer-institut-fuer-sichere-informationstechnologie-cloud-dienste-studie-sicherheit-1.16900343 on 5 August 2014.

119 The debate around the regulation of the taxi service „Uber" documents this nicely, cf. LARRY DOWNES, Lessons from Uber: Why Innovation and Regulation don't mix, Forbes 2013, retrieved from http://www.forbes.com/sites/larrydownes/2013/02/06/lessons-from-uber-why-innovation-and-regulation-dont-mix/ on 5 August 2014; DRUCKER (fn. 103).

120 See further: REHANA HARASGAMA, Compliance multinationaler Unternehmen, Datenschutz im Spannungsfeld sich widersprechender Regulierungen, in: Sandra Brändli/Roman Schister/Aurelia Tamò (eds.), Multinationale Unternehmen und Institutionen im Wandel – Herausforderungen für Wirtschaft, Recht und Gesellschaft, 8. Schriftenreihe der Assistierenden der Universität St.Gallen, St. Gallen 2013, 119 ff.

Representatives of the state and of organizations frequently swap sides. The former German minister of defense Karl Theodor zu Guttenberg, for example, is now consulting the (private) company Ripple Labs.[121] Moreover, organizational representatives try to influence state decisions via lobbying and soft power. Since IT and Internet services are a major part of modern economies, the actors of the exo-system represent a powerful stakeholder in terms of their economic, social and cultural capital.[122]

By setting trends and establishing behavioral mechanisms, organizations change societal norms and consumers often accept these for the sake of convenience (cf. chapter II. A)). In its role as a regulator the state has the challenging task to find the balance between pre-existing norms (e.g. individual privacy), upcoming values (sharing, transparency and convenience), the profit-oriented organizations enforcing these values and the individuals embracing them. The recent Court of Justice of the European Union (CJEU) case of "The Right to Be Forgotten", which has been portrayed and discussed heavily in the public sphere, illuminates these entanglements.

Right to Be Forgotten

The recent CJEU decision on "Google Spain v AEPD and Mario Costeja Gonzalez"[123] illustrates the interactions between the state – or supranational legislators – and the exo-level of organizations. On May 13th, 2014 the CJEU ruled that "*an internet search engine must consider requests from individuals to remove links to freely accessible web pages resulting from a search on their name. Grounds for removal include cases where the search result(s) 'appear to be inadequate, irrelevant or no longer relevant or excessive in the light of the time that had elapsed'*".[124]

This case shows how an interaction between the state – or supranational legislators – and organizations "trickles down" to the individual level and affects the way organizations and individuals interrelate. Although the CJEU's decision affects search engines – and thereby organizations –, the consequences of the decision relate to individuals' concrete online privacy autonomy and constraints. Individuals now have a basis for acting upon perceived privacy infringements in the form of undesired or negative information displayed by

121 WIKIPEDIA, Ripple Labs, retrieved from http://de.wikipedia.org/wiki/Ripple_Labs on 5 August 2014.

122 PIERRE BOURDIEU, Ökonomisches Kapital, kulturelles Kapital, soziales Kapital, Soziale Welt 1983, 183 ff.

123 Case C-131/12, *Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González,* 13 May 2014.

124 Case C-131/12, *Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González,* 13 May 2014.

search engines. Thus, the decision expands their "right to be let alone".[125] At the same time, it does so in a restricted and unbalanced way, since the decision distinguishes between public figures and private persons. As the ongoing discussions about the decision have shown, this is a contested issue by search engines, the press and even legal scholars, since it concerns users' immediate environment but also public interests.[126]

This case is an excellent example for an – at first – abstract and philosophical idea[127] that gains political and practical relevance in a very short time. It documents how organizations must mediate between the interests of the state – protecting citizens from privacy breaches and granting them a right to be forgotten – and its citizens, who may or may not have a (data protection) interest in the information that is supposed to be forgotten.

F) Society – State

Law and regulations reflect ethical principles and moral values of a society at a given time. Privacy is no exception in that regard. Since the moral values between different societies or countries vary vastly,[128] different privacy understandings are at play depending on the country.

For the individual, the interactions between the state, as a concrete actor, and society as an abstraction of norms, myths, and historical imprinting, become relevant at the intersection of public institutions, which symbolize and recreate a society's principles.

125 SAMUEL D. WARREN/LOUIS D. BRANDEIS, The Right to Privacy, Harvard Law Review 1890, 193 ff.

126 See for example: JONATHAN ZITTRAIN, Righting the Right to be Forgotten, retrieved from http://blogs.law.harvard.edu/futureoftheinternet/2014/07/14/righting-the-right-to-be-forgotten/ on 5 August 2014; NORBERT NOLTE, Das Recht auf Vergessenwerden – mehr als nur ein Hype?, NJW 2014, 2238 ff.; House of Lords EU Home Affairs, Health and Education Sub-Committee, Report, retrieved from http://www.parliament.uk/business/committees/committees-a-z/lords-select/eu-home-affairs-sub-committee-f-/news/right-to-be-forgotten-report/ on 5 August 2014; VIKTOR MAYER-SCHÖNBERGER, Omission of search results is not a 'right to be forgotten' or the end of Google, retrieved from http://www.theguardian.com/commentisfree/2014/may/13/omission-of-search-results-no-right-to-be-forgotten on 5 August 2014.

127 VIKTOR MAYER-SCHÖNBERGER, Delete – The Virtue of Forgetting in the Virtual Age, Cambridge 2009.

128 WORLD VALUE SURVEY, retrieved from http://www.worldvaluessurvey.org/WVSContents.jsp on 5 August 2014.

As an example institutions where society and the state interact are courts and public administrations in general. Constitutions, precedent court rulings and national legislation build the legal mechanisms to encode and protect an individual's right to privacy. Through the codification of those moral values and ethical principles regulators are handed the power to act on behalf of citizens and enforce a right to privacy. The ethical value of protecting the private lives, communication and believes of individuals evolved from societal norms to binding (case) law. Philosophers, sociologists, journalists, and legal scholars: all have taken part in the debate and influenced the societal norms.

The example of the EU and Switzerland on the one hand and the United States on the other hand will be employed to illustrate the existing differences in privacy laws emerging from different social norms and values.

Different Conceptions of Privacy: EU vs. US

As the US and Europe have different cultural backgrounds, so do their perceptions of how and at what level privacy should be protected. European law mainly has its roots in German and French culture which are based on a tradition of centralized law-making and self-determination as key aspects to privacy whereas in the US society is based on a strong de-centralization of power and legislation.[129] Thus, there are different ways to implement privacy as a concept in society: The EU and Switzerland follow a so-called *omnibus* data protection approach based on the constitution or in the case of the EU, the ECHR and the CFREU for the EU member states. The misuse of personal data and thereby the infringement of privacy is then protected by the all-encompassing EU Data Protection Directive resp. the Swiss Data Protection Act as a second level of protection. Both pieces of legislation set the minimum standard for the duties and rights of data controllers which include both private persons and the government and the rights of the affected data subjects for all EU and Swiss citizens. These standards include the following principles: collection limitation, data quality, use limitation, purpose specification, security safeguards, openness, individual participation and accountability.[130]

The US, on the other hand, follows a sector- and industry-specific approach, meaning that various, specialized laws regulate privacy protection in a given

[129] JAMES Q. WHITMAN, The Two Western Cultures of Privacy: Dignity Versus Liberty, The Yale Law Journal, Vo. 113, 2004, 1151 ff.

[130] These although more precise are very similar to the OECD Principles presented above in chapter II. D) 2.

sector.[131] This piecemeal approach is one of the reasons why U.S. data protection is known to be very narrow and does not offer the same comprehensive protection as the EU and Switzerland do. Due to these discrepancies and because many companies choose to locate their data mining headquarters in countries with less strict data protection practices and enforcement, the EU as well as Switzerland negotiated the so called Safe Harbor Agreements with the US government. Thereby companies agree to follow the applicable data protection standards when their services are provided to EU or Swiss citizens. On a small scale these agreements attempt to close the gap between the two differing cultural approaches while at the same time addressing the issues the territoriality principle (cf. chapter II. D) 2) raises. Unfortunately, the Safe Harbor Agreements have not proven to be successful in ensuring the same level of data protection on both sides of the Atlantic Ocean.

Besides the omnibus and sector-specific approach – both imply that the government acts as the regulator and enforcer – the industry can act as a regulator itself. Self-regulation initiatives by industry leaders support the normative framework of the macro-level and set industry-wide ethical standards. Such attempts have been seen in the direct marketing industry and reflect societal understandings of privacy within the corporate world.[132] The US is a strong promotes of self-regulation when it comes to privacy.

G) Summary

Table 1 summarizes the intersections between the four layers presented above. It exemplifies the complex interplay of online privacy on different levels. These interactions manifest themselves in specific intersections such as privacy policies, school curricula or legal documents, but they can also be more abstract, for example in the case of organizational identities or political decisions. It is not always possible to clearly restrict interactions to two levels, as they can sometimes entail three or even all four levels of the system. The example of the "Right to be Forgotten" demonstrates such a complex

131 For example, the Health Insurance Portability and Accountability Act (HIPAA) which regulates the use and disclosure of so-called Protected Health Information, the Children's Online Privacy Protection Act (COPPA) which establishes that operators of websites targeted at children under the age of 13 must seek verifiable consent from their parents and restrict the use of data for marketing purposes, or the Video Privacy Protection Act (VPPA) which regulates the use of video rental records.

132 STEPHANIE MILLER, DMA Advocates Self-Regulation of Mobile Marketing, DMA Press Release 2014, retrieved from http://thedma.org/advance/capitol-matters-advocacy-compliance/dma-advocates-self-regulation-of-mobile-technology/ on 2 August 2014.

interaction, where trickle down effects occur and all four levels or layers are somehow involved. In sum, understanding online privacy as a phenomenon that touches different levels and elaborating on the interactions between the layers proves to be a fruitful approach to account for its complexity. Particularly, the dependency and strong ties of the individual (privacy decision) to a broader context of various systems or actors is depicted. Thus, it complements actor-centric views of online privacy with a much needed systemic perspective.

Table 1: Overview of intersections and interactions between the different layers

	Organizations	Society	The State
Individual	*Privacy policies* as a main intersection: organizations with information, expertise and resources benefit; Technological *affordances* and *cyber risks* as further – less visible – intersections.	*Socialization*, experience and learning as important intersections: Privacy norms and values are internalized from the society to the community and rationalized vice versa.	The intersections between the state and individuals are laws, rules, court decisions and – in the case of Switzerland – initiatives and referendums to alter privacy legislation; advocacy and political influence (e.g., Pirate Parties).
Organizations	-	Employee background, organizational values and identity as interaction points.	Laws and regulations as the main point of interaction; monetary interactions occur (taxes) as well as lobbying etc.
Society	-	-	*Institutions* as a main intersection: schools, courts, public administration etc.; via the institutions privacy norms and values "trickle down" to the individual level.

IV. Back to the Future - Concluding Remarks

A) From Framework to the Future

This contribution is the first to analyze information privacy with BRONFENBRENNER'S ecological systems theory. It is also one of the few attempts to systemize the phenomenon of online privacy and consider it from a range of different perspectives with regards to individuals' behavior and management of personal data. So far, most literature on privacy is framed within specific – and often narrow – discourses, shaped by disciplinary positions and boundaries.[134] At the individual level, for example, looking at privacy and disclosure decisions within a privacy calculus framework is a dominant research direction. Therefore, (social) psychology and information systems research have been strong in investigating the individual aspects of online privacy. At the macro-level, by contrast, privacy is understood as a phenomenon to be governed and controlled via legislation, contracts or agreements. Although individual perspectives and problem fields might be involved in adapting the "rules of the game", this discourse on online privacy is different.

Only very few interdisciplinary approaches to the phenomenon exist[135], although several institutions – such as the Berkman Center for Internet and Society or the Oxford Internet Institute – bring together scholars from various disciplines and facilitate the interdisciplinary exchange on online privacy issues. However, such exchange often remains informal, for example in the form of conferences and workshops and seldom finds its way into more structured approaches, such as journal articles, book chapters or project reports. The field and research on privacy is still quite dispersed. Therefore, this contribution is an attempt to structure the field and to approach it within a broad theoretical and interdisciplinary narrative.

Using a multi-layered and interdisciplinary approach proved fruitful in many regards. On the one hand, the phenomenon of information privacy is much more complex as it may appear at first sight, especially when considering works focused on a single layer. Understanding the interplay of the main layers and their dependencies is crucial for the design of well-accepted privacy norms for all involved parties. On the other hand, the proposed framework can guide future research in the operationalization of the privacy phenomenon. When aware of underlying relations and influences, researchers can approach certain aspects of privacy in a more informed manner.

134 SMITH/DINEV/XU (fn. 6)
135 SMITH/DINEV/XU (fn. 6), 1008.

This paper thus makes the claim that future research on privacy should try to operationalize and investigate privacy as a multi-level phenomenon. This is a challenging task, as it entails collecting data in different contexts, from the individual-level, to company-level and country-level and also examining privacy from different perspective within different disciplines.

B) From Framework to Practice

This work is one of the first steps towards a better-informed theoretical and practical approach to privacy. The analysis of interactions between individuals, organizations, society and the state points to different methods on how to handle privacy in the future. Table 2 illustrates the practical recommendations for each interaction level while not attempting to be exhaustive. On the one side, these recommendations are very demanding and not easy to implement; however, they embrace a vision of information privacy as a social value reflected in the actions of individuals, organizations, society and the state.

Table 2: Practical recommendations emerging from the interactions between different layers

	Organizations	State	Society
Individual	Transparent and easy to understand *privacy policies*; literate and educate *users*; Internet companies should be easy (easier) to approach and open for user inputs and concerns; context-aware interfaces and specific solutions for specific groups (e.g., elderly, adolescents etc.) ⇨ Company ethics boards and mechanisms for whistleblowing	Listening to individuals' privacy needs and attitudes; putting privacy on the political agenda; Increasing privacy literacy and knowledge via campaigns or curricula in schools ⇨ Public hearings and political and legal representation of privacy experts in commissions	Media and civil society actors: portraying current developments in a balanced way; sensitizing users about their rights and duties towards the state and organizations when it comes to privacy; shaping individual privacy perceptions
Organizations	-	Regular exchange between regulators and companies to enable a more forward-looking legislation	More reflection on the social implications of the interplay between people and software; more diverse hiring practices; companies should show more engagement and commitment in the public debate
State	-	Legislative adaptions to keep pace with technology (flexibility); protect individuals' privacy and at the same time ensure economic growth and innovation	Accurate adjustment of the regulatory structures, taking into account the country-specific perceptions and concerns towards privacy