ex/ante

Zeitschrift der juristischen Nachwuchsforscher
Revue des jeunes chercheurs en droit
Journal for young legal academics

Ausgabe – numéro – issue 2/2016

Life Sciences

DIKE

Weitere Infos zur Zeitschrift: www.ex-ante.ch

Für Abonnemente und Einzelhefte: verlag@dike.ch

Herausgeber / éditeurs
Stephanie Bernet
Kaspar Ehrenzeller
Gabriel Gertsch
Rehana Harasgama
Nadia Kuźniar
Fiona Savary
Roman Schister

Die Herausgeber danken Eva Cellina herzlich für die Redaktion der französischsprachigen Texte.

Vertrieb und Abonnementsverwaltung / Diffusion et abonnements
Dike Verlag AG
Weinbergstrasse 41, CH-8006 Zürich
Tel. 044 251 58 30, E-Mail verlag@dike.ch, www.dike.ch

Erscheint zweimal pro Jahr (Juni, Dezember) / Parution deux fois l'an (juin, décembre)

Abonnementspreis / Prix de l'abonnement
Jahresabonnement / Abonnement annuel:
CHF 69.– inkl. MWSt/TVA incluse

Jahresabonnement Studierende (bitte Kopie der Legitimationskarte beilegen) / Abonnement annuel étudiants (joindre une copie de la carte de légitimation): CHF 55.– inkl. MWSt/TVA incluse

Die Zeitschrift kann auch als Einzelheft bezogen werden / La revue est également vendue sous forme de cahiers séparés

Kündigungen für die neue Abonnementsperiode sind schriftlich und bis spätestens 31. Oktober des vorangehenden Jahres mitzuteilen. Beanstandungen können nur innert 8 Tagen nach Eingang der Sendung berücksichtigt werden. Für durch die Post herbeigeführte Beschädigungen sind Reklamationen direkt bei der Poststelle am Zustellort anzubringen.

La résiliation de l'abonnement pour une nouvelle période doit être communiquée par écrit au plus tard jusqu'au 31 octobre de l'année précédant la nouvelle période. Seules les réclamations faites dans les huit jours dès réception du numéro seront prises en compte. Les réclamations relatives aux dommages causés par les services postaux doivent être directement adressées à l'office postal de distribution.

Weitere Informationen zur Zeitschrift, Inserate-, Unterstützungs- und Publikationsmöglichkeiten finden Sie unter www.ex-ante.ch.

Vous trouverez plus d'informations sur la revue, l'insertion d'annonces ainsi que les possibilités de soutien et de publication sur www.ex-ante.ch.

ISSN 2297-9174
ISBN 978-3-03751-879-3

Inhaltsübersicht / Sommaire

Privacy through Multiple Lenses: Applying the St. Galler Privacy Interaction Framework (SG-PIF)

Christoph Lutz* / Pepe Strathoff** / Aurelia Tamò*** / Flavius Kehr****

KEYWORDS privacy, email tracking, ethics, systemic perspective

ABSTRACT This article revisits the St. Galler Privacy Interaction Framework (SG-PIF) and applies the framework to email tracking. The SG-PIF conceptualizes privacy on different levels and investigates the interaction between individuals' privacy behavior and their environment on four layers: the personal level, organizations, society, and the government.

ZUSAMMENFASSUNG Dieser Artikel erläutert das St. Galler Privacy Interaction Framework (SG-PIF) und wendet die Theorie auf eine Fallstudie zu Email-Tracking an. Das SG-PIF beschreibt Privacy-Handlungen als ein Phänomen auf mehreren Ebenen: der persönlichen Ebene, der Organisationsebene, der Gesellschaft und der Regierung.

RÉSUMÉ Cette article décrit le St. Galler Privacy Interaction Framework (SG-PIF) et applique cette théorie en décrivant le phénomène de «email tracking». Le SG-PIF conceptualise la notion de «privacy» (la vie privée) en analysant quatre facteurs qui influencent la vie privée: les individuels, les organisations, la société et le gouvernement.

I. Introduction

Nearly all internet services and applications that simplify everyday life collect and store private information, including sensitive data such as personal preferences, health and location information, or financial information such as bank account or credit card numbers. Given the huge amount of accessible and exploitable data collected by private and public actors alike, the provision of personal information has raised severe concerns on potential misuse or loss of data.

As such, scholars from various fields have attempted to describe and explain phenomena related to data privacy in the information age. Consequently, different understandings of the nature of privacy exist, ranging from economic and psychological[1] to legal[2] or philosophical perspectives.[3] Moreover, researchers have repeatedly alluded to the multi-dimensionality of the privacy construct.[4] Bélanger/Crossler, for example, suggested that privacy concerns may result from complex interactions on different levels, such as government, society, or the economy, while Smith/Dinev/Xu emphasized the role of culture as a predictor of individual privacy beliefs and attitudes.[5] Still, research adopting 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.

The main goal of this paper is to explore the potential of a model aiming to fill this research gap: The St. Gallen Multi-Layered Privacy Interaction Framework (SG-PIF). We chose email tracking to illustrate the multidimensional structure of privacy by means of the SG-PIF. In general,

* Christoph Lutz, PhD, Ass. Prof. BI Norwegian Business School.
** Pepe Strathoff, PhD, Fellow at the Center for Leadership and Values in Society, University of St. Gallen.
*** Aurelia Tamò, PhD candidate, University of Zurich.
**** Flavius Kehr, PhD, University of St. Gallen.

1 Cf. here in particular Kai-Lung Hui/I. P. L Png, The Economics of Privacy, in: Hendershott (ed.), Handbooks in Information Systems: Economics and Information Systems, Bingley 2006, 471 et seq.; Christopher Kuner/Fred Cate/Christopher Millard/Dan Jerken Svantesson, The Challenge of Big Data for Data Protection, International Data Privacy Law, 2012, 2(2), 47 et seq.; Shivendu Shivendu/Ramnath Chellappa, An Economic Model of Privacy: A Property Rights Approach to Regulatory Choices for Online Personalization, Journal of Management Information Systems 2007, 24(3), 193 et seq.

2 Paul Bender, Privacies of Life, Harper's Magazine 1974, 123(4), 36 et seq.; Samuel Warren/Louis Brandeis, The Right to Privacy, Harvard Law Review 1890, 4(5), 193 et seq.

3 Cf. here in particular Irwin Altman, The Environment and Social Behavior: Privacy, Personal Space, Territory, and Crowding, Monterey 1975; Paul Pavlou, State of the information privacy literature: where are we now and where should we go? MIS Quarterly 2011, 35(4), 977 et seq.

a case study approach seems appropriate, as the multi-layered perspective on privacy requires analyzing the phenomenon from a rather holistic perspective. Moreover, Darke/Shanks/Broadbent point out that the case study method is especially popular among researchers who investigate interactions between technological innovations and organizational/social contexts[6], and choosing cases that are unique and special is a common approach for case selection proposed by Yin in his seminal book on the case study method.[7] However, it should be emphasized that the case study in this paper mainly serves to illustrate the possibilities of the SG-PIF with regard to its potential to structure complex privacy phenomena and not to actually test or develop a theory.

The paper is structured as follows: After the Introduction (section 1), we briefly give an overview of online privacy theories, introduce the SG-PIF and discuss its basic outlines (section 2 and 3). Then, we look at email tracking as an example of current organizational practices that individuals may be unaware of (section 4). As outlined above, the case study was chosen to illustrate the potential usefulness of the SG-PIF for a wide range of privacy-related phenomena. Finally, we conclude the paper with a summary, the implications and the limitations of our approach (section 5).

II. A short overview of online privacy theories

As indicated in the introduction, privacy is a complex topic, with a range of interpretations and a multitude of scientific disciplines involved in its study. Consequently, a vast body of literature on the topic exists. Several valuable theories have been developed to analyze privacy in digital contexts. In this article, we focus on social science theories and give an overview of four prominent approaches: communication privacy management[8], privacy as contextual integrity[9], privacy by design[10], and the privacy paradox literature[11]. We will then discuss shortcomings of these approaches that call for a more holistic privacy theory. Our interest here is mainly on informational privacy, not so much on physical, social and psychological privacy, although the different forms are often not clearly separable.

Communication privacy management theory (CPM) was developed by Petronio and is an attempt to understand individuals' private information disclosure.[12] According to Petronio, individuals establish privacy boundaries by carrying out a «mental calculus» to evaluate the type and amount of private information they share with others. Over time, actors develop privacy rules that govern how much private information they want to share with different people in their social environment. Once private information has been disclosed, the recipients become co-owners of this information. Thus, CPM sees self-disclosure as a dyadic and not as a one-dimensional process. However, one of the core tenets of CPM is that individuals think they have a right to own and control their personal information (even after it has been shared with others). The concept of privacy boundaries denotes «borders of ownership surrounding private information».[13] Privacy boundaries vary in their strictness and can range from thick (for confidential information such as secrets) to thin (for less confidential information such as someone's profession). When privacy rules are violated, privacy turbulences occur and existing privacy rules need to be recalibrated or new ones established. CPM was expanded over time and contains a set of axioms that aptly describe the theory.[14] For example, the core tenet of pri-

4 Jeff Smith/Tamara Dinev/Heng Xu, Information privacy research: An interdisciplinary review, MIS Quarterly 2011, 35(4), 989 et seq.

5 France Bélanger/Robert Crossler, Privacy in the Digital Age: A Review of Information Privacy Research in Information Systems, MIS Quarterly 2011, 35(4), 1017 et seq.; Smith/Dinev/Xu (Fn. 4), 989 et seq.

6 Peta Darke/Graeme Shanks/Marianne Broadbent, Successfully completing case study research: combining rigour, relevance and pragmatism, Information Systems Journal 1998, 8(4), 273 et seq.

7 Robert Yin, Case Study Research: Design and Methods, Los Angeles 2009.

8 Cf. in particular Sandra Petronio, Boundaries of privacy: Dialectics of disclosure, Albany 2002.

9 Cf. here in particular Helen Nissenbaum, Privacy as Contextual Integrity, Washington Law Review 2004, 79, 101 et seq.

10 Cf. here in particular Ann Cavoukian, Privacy by Design – The 7 Foundational Principles. Information and Privacy Commissioner of Ontario, 2009, Retrieved from https://www.iab.org/wp-content/IAB-uploads/2011/03/fred_carter.pdf, last visited June 15, 2016.

11 Cf. here in particular Susan Barnes, A privacy paradox: Social networking in the United States, First Monday 2006, 11(9), Retrieved from http://firstmonday.org/article/view/1394/1312, last visited June 15, 2016; Ralph Gross/Alessandro Acquisti, Information revelation and privacy in online social networks, Proceedings of the 2005 ACM workshop on Privacy in the electronic society, 71 et seq.

12 Petronio (Fn. 8); cf. also her earlier work Sandra Petronio, Communication boundary management: A theoretical model of managing disclosure of private information between marital couples, Communication Theory 1991, 1(4), 311 et seq.

13 Sandra Petronio/Wesley T. Durham, Communication Privacy Management theory: Significance for interpersonal communication, in: Baxter/Braithwaite (eds.), Engaging theories in interpersonal communication: Multiple perspectives, London 2015, 335 et seq., cf. 338.

14 Petronio/Durham (Fn. 13), 335 et seq.

vate information control is shaped by individuals' privacy rules. These rules, in turn, vary depending on a range of factors such as the cultural context, gender and the situational context. Being a communication theory[15] at its core, CPM has been frequently applied in communication research. In particular, CPM has proven to be valuable in the investigation of interpersonal communication in family settings and online communication.[16]

Nissenbaum's notion of *contextual integrity* accounts for context-specific privacy.[17] Contextual integrity describes an approach where data collecting entities respect the privacy norms in a given context – instead of collecting data on a «catch-it-all»-basis. Thus, privacy is secured as long as data collectors fulfill the norms of appropriateness (what constitutes private information in a given situation) and distribution (how and to whom should information be given in a certain context). In practical terms, this includes an understanding of these two norms in the application domain of a certain technology. For example, some social media apps such as Snapchat are used to share private information, where appropriately shared information between communication partners is broad and can include sensitive images, secrets and profound emotions. By contrast, professional social media such as LinkedIn present a context where appropriate information is much more restricted, e.g., to relevant news, new jobs and appointments or professional networking. It does not make sense to apply the same privacy expectations and norms to Snapchat and LinkedIn.

A third approach to privacy that tackles the topic with more applied objectives in mind is *privacy by design*. Cavoukian, as a key proponent of this line of thinking, argues, «privacy must be incorporated into networked data systems and technologies, by default. Privacy must become integral to organizational priorities, project objectives, design processes, and planning operations. Privacy must be embedded into every standard, protocol and process that touches our lives.»[18] Privacy by design is a holistic approach including the employment of privacy-friendly information technology (such as the use of privacy-enhancing technologies), measures on an organizational level (e.g., management support for privacy) and on a physical level (e.g., access controls). The concept aims at breaking up vague philosophical principles of privacy into different patterns.[19] Transparency of the data evaluation, for example, is a central cornerstone for privacy-friendly devices. Transparency can be broken down into elements such as defining and articulating which data is being processed, when data is erased from a server, how users can control data, or object to processing it at all. According to privacy by design, regulators should split the general data protection and privacy principles into smaller units, use terminologies employed in other disciplines such as computer science, find the ontologies and taxonomies within them, and provide regulation that is more flexible. Once this is done, more tangible sub-rules can be formulated and implemented on a case-by-case-basis.

The question why users choose to disclose significant amounts of personal data on the internet despite reporting privacy concerns has long been at the heart of privacy research. The concept of a *privacy paradox*, initially formulated by Barnes to define the perplexing divide between privacy-concerned adults and self-disclosing digital teenagers[20], has evolved to incorporate discrepancies between individual attitudes and behavior when it comes to (online) privacy[21]. A number of studies have found privacy concerns (attitude) to exert only a weak, if any, effect on online self-disclosure or protective behavior (behavior).[22] The empirical evidence on the privacy paradox is as mixed as are the existing theoretical perspectives.[23] While older studies tend to confirm the paradox, newer analyses often find a significant effect of privacy concerns on privacy protection behavior or self-disclosure online, thus rejecting the paradox. Scholars have developed several interpretations to explain the privacy paradox. One of the most prominent explanations is based on the thought of a privacy calculus.[24] According to this idea, individ-

15 Petronio/Durham (Fn. 13), 335 et seq.

16 Cf. Kail Ryan Steuber/Denise Haunani Solomon, Relational uncertainty, partner interference, and privacy boundary turbulence: Explaining spousal discrepancies in infertility disclosures, Journal of Social and Personal Relationships 2012, 29(1), 3 et seq.; Maggie Kanter/Tamara Afifi/Stephanie Robbins, The impact of parents «friending» their young adult child on Facebook on perceptions of parental privacy invasions and parent–child relationship quality, Journal of Communication 2012, 62(5), 900 et seq.

17 Cf. here Nissenbaum (Fn. 9), 101 et seq.

18 Cavoukian (Fn. 10).

19 Cavoukian (Fn. 10).

20 Barnes (Fn. 11).

21 Zeynep Tufekci, Grooming, gossip, Facebook and MySpace: What can we learn about these sites from those who won't assimilate?, Information, Communication & Society 2008, 11(4), 544 et seq.

22 Cf. for an overview over privacy paradox research: Tobias Dienlin/Sabine Trepte, Is the privacy paradox a relic of the past? An in-depth analysis of privacy attitudes and privacy behaviors, European Journal of Social Psychology 2015, 45(3), 285 et seq.; Spyros Kokolakis, Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon, Computers & Security, 2015.

23 Kokolakis (Fn. 22).

24 Tamara Dinev/Paul Hart, An extended privacy calculus model for e-commerce transactions, Information Systems Research 2006, 17(1), 61 et seq.

uals make rational decisions about disclosing personal information on the internet by weighing the benefits of disclosure against its costs and potential risks.[25] Other explanations include trust[26], the distinction of community and society *(Gemeinschaft* and *Gesellschaft* according to Tönnies' dichotomy)[27], the differentiation between social and institutional privacy threats[28], and privacy awareness and literacy.[29]

None of these four approaches provides a holistic theory of privacy and each one has shortcomings. CPM and the privacy paradox literature often neglect organizational aspects and individuals' embeddedness into organizations and institutions such as companies, schools, voluntary associations and social milieus more broadly. Contextual integrity and privacy by design, on the other hand, see privacy as a context-specific phenomenon. In contrast to CPM and the privacy paradox literature, however, these approaches tend to not include individual decision-making processes and heuristics. Moreover, the approaches discussed here largely fail to address the role of regulation and the government in individuals' privacy decisions. Finally (and except for privacy by design), these approaches are not very sensitive to technological characteristics and how they might influence users' privacy behavior. In the next section, we propose some building blocks for a holistic theory of privacy that strives to overcome some of these shortcomings.

III. The multi-layered privacy interaction framework (or the St. Galler Privacy Interaction Framework)

The SG-PIF was developed by an interdisciplinary team of researchers in 2014 and 2015.[30] The goal of the SG-PIF is to understand and analyze online privacy as a multi-dimensional – and thus multi-disciplinary – phenomenon. Such a systemic perspective goes beyond the individualistic view in psychological research on online privacy on the one hand and supersedes the focus on macro developments as present in legal, philosophical, and ethical approaches to online privacy on the other hand. It integrates various layers of users' social reality and includes differing levels of abstraction.

The SG-PIF relies on Bronfenbrenner's ecological model of human development.[31] The model understands individuals as constantly interacting with various spheres or systems of the social environment. Bronfenbrenner distinguishes several systems with increasing distance from the individual: interactions between individuals and their immediate environment are called *micro-systems*. In turn, social groups without immediate contact with the individual, such as neighbors or parental workplaces, belong to the *exo-system*. Relations between social groups characterized by a large proximity to the individual (such as parents interacting with a child's school) are considered *meso-systems*. Finally, *macro-systems* refer to the structure in which all other systems are embedded. Hence, the macro-system entails laws, traditions and values of a whole society.[32]

The SG-PIF uses the basic idea of Bronfenbrenner's model – the division of the social environment into different systems – as the starting point to conceptualize online privacy as a multi-dimensional phenomenon. However, we adapted Bronfenbrenner's model to meet the specific context of online privacy.[33] Figure 1 depicts the basic structure of the SG-PIF.

---

25 Haein Lee/Hyejin Park/Jinwoo Kim, Why do people share their context information on Social Network Services? A qualitative study and an experimental study on users' behavior of balancing perceived benefit and risk, International Journal of Human-Computer Studies 2013, 71(9), 826 et seq.

26 Hanna Krasnova/Sarah Spiekermann/Ksenia Koroleva/Thomas Hildebrand, Online social networks: why we disclose, Journal of Information Technology 2010, 25, 109 et seq.

27 Cf. on the dichotomy: Christoph Lutz/Strathoff Pepe, Privacy Concerns and Online Behavior – Not So Paradoxical After All? Viewing the Privacy Paradox through Different Theoretical Lenses in Brändli/Schister/Tamò (eds.), Multinationale Unternehmen und Institutionen im Wandel – Herausforderungen für Wirtschaft, Recht und Gesellschaft, Bern 2013, 81 et seq.; Pepe Strathoff/Christoph Lutz, Gemeinschaft schlägt Gesellschaft: Die vermeintliche Paradoxie des Privaten, in Hahn/Hohlfeld/Knieper (eds.), Digitale Öffentlichkeit(en.) Schriftenreihe der DGPuK, Band 42, 2015, 203 et seq.

28 Alyson Leigh Young/Anabel Quan-Haase, Privacy protection strategies on Facebook: The Internet privacy paradox revisited. Information, Communication & Society 2013, 16(4), 479 et seq.

29 Miriam Bartsch/Tobias Dienlin, Control your Facebook: An analysis of online privacy literacy. Computers in Human Behavior, 2016, 56, 147 et seq.

30 Lea Aeschlimann/Rehana Harasgama/Flavius Kehr/Christoph Lutz/Veselina Milanova/Severina Müller/Pepe Strathoff/Aurelia Tamò, Re-Setting the Stage for Privacy: A Multi-Layered Privacy Interaction Framework and Its Application, in: Brändli/Harasgama/Schister/Tamò (eds.), Mensch und Maschine – Symbiose oder Parasitismus?, Bern 2015, 1 et seq.

31 Urie Bronfenbrenner, Toward an experimental ecology of human development, American Psychologist 1977, 32(7), 513 et seq.

32 Bronfenbrenner (Fn. 31), 513 et seq.

33 Aeschlimann/Harasgama/Kehr/Lutz/Milanova/Müller/Strathoff/Tamò (Fn. 30), 1 et seq.

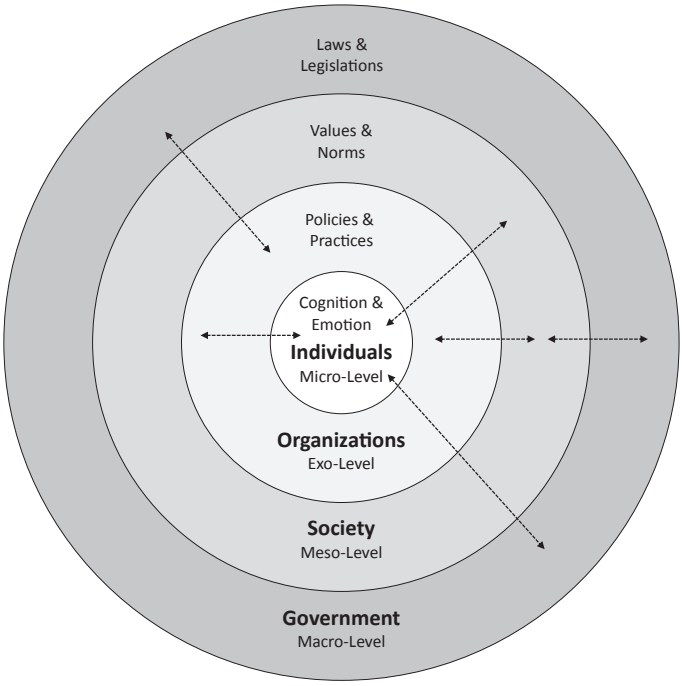

Figure 1. *The multi-layered privacy interaction framework (SG-PIF).*

Following Bronfenbrenner's ecological model, we assume that individual privacy considerations are influenced by (1) individual cognitions and emotions at the micro-level, (2) stakeholders dealing with personal data, such as online service providers (Google, Facebook, Amazon etc.) and non-profit organizations, at the exo-level, (3) social norms and values indirectly guiding individual decision-making at the meso-level, and (4) governmental decisions, regulations and laws at the macro-level. Thus, we distinguish the following aspects as relevant for an individual's privacy considerations: (1) individuals, (2) organizations, (3) society and (4) the government. Privacy is rooted in all those layers and privacy-related interactions between the different layers will affect individual decisions on information disclosure. These interactions are crucial to understanding online privacy. For example, in the context of social networking sites, the micro-level of individual cognitions and emotions and the exo-level of organizational stakeholders interact via privacy policies and agreements. Neglecting the multi-layered nature of online privacy and the interactions between the system layers, leads to a one-sided and biased understanding of why individuals act the way they do when it comes to online privacy. In the following chapter, we apply the SG-PIF to email tracking. This case study attempts to demonstrate the usefulness of conceptualizing online privacy as a multi-layered phenomenon.

IV. Case study: Email tracking

The term email tracking describes the practice of including so-called tracking elements in newsletter emails, which can be used to track if, when, where and with which device a recipient reads an email. Tracking elements are personalized links or little pictures (most often invisible to the user) which are activated once an email has been opened. Linked to user information (e.g., a user's email address or online profile), they allow the sender to collect personalized information about a particular consumer. A recent study with data from Germany found that nearly all newsletter emails include at least one tracking element.[34] While businesses may have a clear interest in such personalized information, given that customer data is of increasing importance to business success[35], users might not want firms to know where they are, which devices they use and when they check their emails. As such, this conflict of interests and the prevalence of the practice underlines that the topic is worth studying and suitable for applying the SG-PIF.

34 Benjamin Fabian/Benedict Bender/Lars Weimann, E-Mail Tracking in Online Marketing – Methods, Detection, and Usage, in Proceedings of the 12, International Conference on Wirtschaftsinformatik 2015, 1100 et seq.

35 Avi Goldfarb/Catherine Tucker, Shifts in Privacy Concerns, American Economic Review 2012, 102(3), 349 et seq.

The SG-PIF is organized around the idea of individual privacy decisions at the micro-level. From this perspective, one may wonder whether, why and under which circumstances individuals are willing to give up their privacy by sharing personal information. While established models of privacy decision-making[36] make the assumption that individuals fully anticipate and trade-off privacy risks and benefits prior to data disclosure, they also presume thate individuals are aware that their data is being collected and thus, know the consequences. In the case of email tracking, however, individuals may not be aware that they are disclosing private information about themselves by simply opening an email. Consequently, the important question is not why individuals disclose private information, but why users open certain newsletter emails as opposed to others. Hence, the persuasive characteristics of the sender (known, trusted, interesting emails in the past, etc.) and the subject line (potentially interesting information, special offers, etc.) come into play.[37]

Closely linked to this argument, the way organizations design their services is of high importance.[38] In the SG-PIF, such organizational influences and practices are represented at the exo-level. With regard to email tracking, firms might be more or less transparent about the use of such techniques. In addition, different uses of the collected data are possible: For instance, firms might only use the data for internal purposes such as tailoring their offers to consumers and targeted advertising. However, they might also sell the data to external data brokers who deal with huge amounts of personal data without the public taking notice.[39] Apart from the senders of such emails, providers of mailing software constitute a second instance of organizations that are involved in email tracking practices. That is, settings of email software determine whether tracking links are activated or not. Some email providers block external pictures in emails, unless the user activates them. In this case, the receiver of the email does not disclose information to the sender, as the tracking pictures are not downloaded. Therefore, providers may actively regulate email tracking by deploying filtering algorithms, and thereby reduce the likelihood of an email affecting a user's privacy.

At the same time, email tracking practices of organizations are highly influenced by a society's cultural and moral values and norms. That is, a firm may be less likely to be opaque with regard to data collection and use if a society strongly rejects such practices, while an email provider may be more likely to deploy blocking techniques if a society encourages such actions. Societal and cultural values are represented at the meso-level of the SG-PIF. In this regard, it is assumed that values and norms of a society may influence privacy attitudes and therefore, determine whether emails are seen as a form of sealed, private message or whether tracking is broadly accepted as a handy way for firms to tailor their offerings to users' preferences.[40] From this viewpoint, one must also consider that privacy does not exist per se, but is a socially construed space to protect individual information.[41] Therefore, privacy is permanently (re-)negotiated and (re-)defined in different societies. As a consequence, email tracking may be considered legitimate in certain countries or cultures but not in others, while societal attitudes about the legitimacy of email tracking can also change over time.

Legislation and governmental decisions on privacy, in turn, are represented on the macro-level of the SG-PIF. Due to its role as a regulator, the government is important as it can put in place legislation that bans or fosters privacy practices.[42] In the case of email tracking, this can be done by specific regulation which is directly targeted at email tracking or via a more general right to privacy that might be enshrined in a country's constitution. In the latter case, it is up to interpretation whether email tracking violates individuals' right to privacy. The role of the government seems to be especially important for the issue of email tracking, because individuals do not make a conscious decision to disclose their data in exchange for something else, but have invisible tracking technologies «crawl» their inboxes. Where individuals cannot protect themselves,

---

36 Such as the privacy calculus, cf. Flavius Kehr/Tobias Kowatsch/Daniel Wentzel/Elgar Fleisch, Blissfully ignorant: The Effects of General Privacy Concerns, General Institutional Trust, and Affect in the Privacy Calculus, Information Systems Journal 2015, 25(6), 607 et seq.

37 Cf. here Christian Hoffmann/Christoph Lutz/Miriam Meckel, Digital Natives or Digital Immigrants? The Impact of User Characteristics on Online Trust, Journal of Management Information Systems 2014, 31(3), 138 et seq.

38 Paul Benjamin Lowry/Greg Moody/Anthony Vance/Matthew Jensen/Jeff Jenkins/Taylor Wells, Using an elaboration likelihood approach to better understand the persuasiveness of website privacy assurance cues for online consumers, Journal of the American Society for Information Science and Technology 2012, 63(4), 755 et seq.; Mary Culnan/Cynthia Clark Williams, How Ethics Can Enhance Organizational Privacy: Lessons from the Choicepoint and TJX Data Breaches, MIS Quarterly 2009, 33(4), 673 et seq.

39 CBS News, The Data Brokers: Selling your personal information, 2014. Retrieved from www.cbsnews.com/news/the-data-brokers-selling-your-personal-information, last visited June 15, 2016.

40 James Moor, Towards a Theory of Privacy in the Information Age, Computers and Society 1997, 27(3), 31 et seq.

41 Moor (Fn. 40), 31–34.

42 Cf. e.g., Daryl Nord/Tipton McCubbins/Jeretta Horn Nord, E-Monitoring in the Workplace: Privacy, Legislations, and Surveillance Software, Communications of the ACM 2006, 49(8), 72 et seq.

the government might step in by enacting laws that give users the sovereignty over their data. This does not necessarily mean that email tracking is banned, but could also take the form of requiring senders of newsletter emails to inform users if tracking elements are included and what will happen with their data once collected.

As outlined above, email tracking represents a complex multi-dimensional phenomenon that requires extensive examination from different perspectives. For scientists and practitioners, the SG-PIF may serve as a framework to deliberate causes and consequences of such practices and to think through the complex dynamics that result from changes on one level. For example, raising individual awareness on privacy issues on the micro-level may influence societal values (meso-level) as a whole, thus affecting legislation (macro-level) and organizational practices (exo-level). With regard to email tracking, one may therefore expect more restrictive legislation that confines opaque tracking practices of firms if (1) individual awareness on email tracking is raised and (2) a majority of individuals in a society starts to condemn these practices as unethical. There are examples for such developments in different areas – for example, the increasing number of confidence tricks on e-commerce websites has led German policy-makers to enact legislation that prescribes e-commerce firms to explicitly inform consumers about purchasing costs by labeling buttons accordingly (e.g., «order with costs», BGB 2012). At the same time, email software providers may have the power to accelerate these sort of developments by fostering the spread of blocking and filtering algorithms. That is, one may assume individual awareness on email tracking to increase if providers comprehensively warn consumers about such practices prior to displaying an email. As such, organizational practices at the exo-level may not only constitute passive playthings for changing societal values and legislation, but may also influence and shape individual decision-making as well as societal attitudes in a direct and active manner. Also, initiatives by governmental organizations on a macro-level may contribute to changing individual and societal attitudes. For example, publishing lists of companies that use email tracking to collect personalized information might lead individuals to decide not to subscribe to certain newsletters, undermining the effectiveness of such practices from the organizational perspective. Yet, the reverse might be possible as well: Consumers might not really care about their privacy and freely disclose any information that can be collected with tracking elements. Organizations at the exo-level might benefit from this development by creating revenue from user data, while policy-makers might not attempt to regulate the market that arises from email tracking practices.

V. Discussion and Conclusion

In this article, we attempted to demonstrate how the SG-PIF can be applied to current privacy-related phenomena to entangle complex privacy situations. This contribution points out that we need to go beyond an individualistic and psychological understanding of privacy, which only considers individual decision-making. Furthermore, it reminds us that a legalistic, regulatory approach without considering organizational, cultural or personal needs cannot do justice to today's complex online privacy landscape. Instead, a systemic perspective, as proposed by the SG-PIF, may help to entangle the multitude of stakeholders involved in online privacy and show how different interests and systems interact.

Analyzing online privacy with the SG-PIF has several advantages as well as theoretical and practical *implications*. The SG-PIF provides guidance on how to systematize and analyze the different perspectives as well as the potentially conflicting interests at play when dealing with technological changes that impact the privacy of individuals. For example, organizations may be interested in collecting as much data as possible in order to develop more advanced technological solutions, or more diverse business opportunities (such as selling email data). However, this thirst for data might not match individual privacy attitudes or societal values and norms. Governmental institutions, on the other hand, have to carefully ponder these conflicting interests and find legal solutions that meet the expectations of individuals while not overly restricting organizational interests. Given this area of conflict, the SG-PIF serves as a helpful framework to structure discourses on privacy. This is especially true for technological developments that impact informational privacy in a holistic manner.

The case study reveals some concrete implications: First, the conflict potential between actors at different levels of abstraction (or in different systems) became apparent. Thus, we saw a stark contrast between users who do not want to be tracked, and companies that apply tracking to a large extent and take advantage of an ambiguous regulatory situation. The use of the SG-PIF shed light on how trust matters when it comes to online privacy, especially when the exo-system of organizations is involved.[43] As such, the SG-PIF provided a relational understanding of privacy where different layers interact systematically.

43 Lutz/Strathoff (Fn. 27), 81 et seq.

In terms of the *practical implications*, the SG-PIF provides careful suggestions on how to unite the different stakeholders involved in privacy management.[44] In this regard, one important notion refers to privacy knowledge or privacy literacy.[45] That is, a basic awareness of online privacy (e.g., how companies track, filter and process personal information) as well as certain skills for data protection should be promoted by schools, the media and politics. This could be done by putting privacy literacy on school curricula and offering accessible online courses, tutorials, or videos dealing with the topic. Another aspect revolves around feasible privacy policies that align the needs of users and engineers.[46] Finally, there need to be spaces where actors from different systems come together for productive knowledge exchange on privacy.[47] Initiatives in the domain of open data or the *WebWeWant* initiative (https://webwewant.org/) by Tim Berners-Lee and colleagues seem to be promising avenues in this area.

While the SG-PIF has the potential to advance the understanding of online privacy, several *limitations* need to be noted. First, the SG-PIF constitutes a systemic approach to privacy. While such an approach may comprise many advantages with regard to its ecological validity and explanatory power for real-life phenomena, it may be difficult to implement the SG-PIF in empirical studies that strive for high internal validity and doubtless cause-consequence relationships. This aspect becomes even more crucial when regarding the interdisciplinary, boundary-spanning nature of the SG-PIF that touches on very different research and methodological paradigms: For example, studies that aim to investigate the individual layer (micro-level) of the SG-PIF might be best suited within a psychological research tradition where experiments, surveys, and interviews are most prevalent. For the meso-system, in contrast, comparative designs might be most suitable. For the exo-system, methods commonly used in organizational (behavior) research, such as case studies and expert interviews prevail. Finally, to investigate the macro-system of online privacy, researchers might rely on (comparative) legal analysis or historical studies with archival data. Combining such a diversity of methods poses a complex challenge and requires a carefully planned research concept and design. Future studies that aim to assess the SG-PIF in an empirical way should thus include a multi-disciplinary research team with experience in a large range of methodological approaches and traditions. Conceptual limitations of the SG-PIF concern the under-specification of interactions with more than two main systems involved. Future research could develop more fine-grained analytical prescriptions on trickle-down effects – spreading from macro, to meso, exo, and micro – as well as bottom-up diffusion – starting from small-scale micro initiatives to exo, meso, and macro ones. Besides, the SG-PIF was designed as a framework to discuss and explain the reactions towards technology rather than the technology itself, resulting in the question on whether and how technology as a main source of privacy issues should be inserted in the model. That is, technology could be regarded as a fifth layer that drives and changes individual decisions, organizational practices, societal values and government policies, but may be also impacted by them.

Overall, however, the SG-PIF represents a useful approach to understanding online privacy as it guides and schematizes the discussion allowing the comparison of scenarios and developments. This paper has illustrated this potential by focusing on email tracking as a newer phenomenon and its privacy-related impacts on the various layers and the interaction between those layers. Thereby, this article contributes to the analysis of complex privacy phenomena. Advances in technology will further drive the importance of privacy-related issues that will have to be addressed by individuals, firms, societies, and public policy makers alike. In this paper, we attempted to contribute to this ongoing debate.

---

44 Aeschlimann/Harasgama/Kehr/Lutz/Milanova/Müller/Strathoff/Tamò (Fn. 30), 1 et seq.

45 Sabine trepte/Doris teutsch/Philipp K. Masur/Carolin Eicher/Mona Fischer/Alisa Hennhöfer/Fabienne Lind, Do People Know About Privacy and Data Protection Strategies? Towards the «Online Privacy Literacy Scale», in Gutwirth/Leenes/De Hert (eds.), Reforming European Data Protection Law, Amsterdam 2015, 333 et seq.

46 Cavoukian (Fn. 10).

47 Strathoff/Lutz (Fn. 27), 203 et seq.