Privacy Concerns and Online Behavior – Not so Paradoxical After All?

Viewing the Privacy Paradox through different theoretical lenses

CHRISTOPH LUTZ / PEPE STRATHOFF

Table of Contents

I.	Introduction.....	81
II.	Theoretical Background and Literature Review	83
	A) Privacy Paradox.....	83
	B) Explaining the Privacy Paradox	84
III.	Methods and Results.....	89
	A) Data and Sample.....	89
	B) Descriptive Part.....	90
	C) Explanatory Part.....	91
IV.	Discussion	93
V.	Conclusion	97

I. Introduction

Recent scandals have sparked the public discussion about online privacy. Since Edward Snowden's release of secret information on the PRISM program many people question the possibility of controlling personal data. It has led to shock, outrage and cynicism. Seemingly, secret services can collect sensitive information about citizens in previously unimaginable ways – «thanks» to the co-operation of Internet companies such as Facebook and Google.

The convenience of web services and people's frequent use of them stand in stark contrast to their downsides: being traceable, becoming the target of personalized advertising, losing spontaneity and serendipity¹, and being exposed to boring, stupid memes, and bland status updates.

¹ ELI PARISER, The Filter Bubble, 1st ed., New York 2011.

At this point in time, the parallelism of promises and good affordances of the web on the one hand (the good net), and disappointments as well as dark sides on the other hand (the bad net) might be as pronounced as never before². This contrast is reflected by the privacy paradox. Many Internet users embrace online services like never before but still worry about the risks and negative consequences. The urge of profiting from the opportunities of the web seems to outweigh the concerns.

This contribution aims to provide a new avenue to understanding the privacy-paradox. Our approach rests on research in online trust and on the theory of public value³ as well as TÖNNIES duality of *Gemeinschaft* and *Gesellschaft*⁴. We show with representative data from 2012 that the very providers of Internet and mobile services – web companies and telecommunication providers (telcos) – enjoy very low levels of trust in terms of privacy protection. Even before the PRISM scandal Swiss people distrusted these organizations. By contrast, financial institutions, the public service, and government enjoy high levels of (data protection) trust.

In terms of the explanatory results, we first look at the privacy paradox in its original conceptualization, as a trade-off between attitudes (as privacy concerns) on the one hand and behavior on the other. In our case, there is a weak but significant influence of concerns on behavior, rejecting the paradox in this form. Swiss users with strong online privacy concerns are slightly but significantly more likely to protect themselves online, e.g. by using encrypted search engines.

In a second step, we investigate the privacy paradox as a trust paradox – as a trade-off between attitudes as trust towards Internet companies and telcos on the one hand and behavior on the other. This time, the paradox is evident, because low trust levels do not result in protective behavior in terms of privacy and security. Thus, the privacy paradox in Switzerland is a trust problem rather than a concern problem. We rely on public value theory, research on trust and the duality of *Gemeinschaft* and *Gesellschaft* to explain the findings and to get a better understanding of the privacy paradox.

This contribution proceeds in four steps. First, a theoretical background on privacy, trust and public value is given and the relevant literatures are briefly re-

² ERIC M. USLANER, Trust, Civic Engagement, and the Internet, *Political Communication* 2004, 2, 223 ff.

³ TIMO MEYNHARDT, Public Value Inside: What is Public Value Creation? *International Journal of Public Administration* 2009, 3–4, 192 ff.

⁴ FERDINAND TÖNNIES, *Studien zu Gemeinschaft und Gesellschaft*, Wiesbaden 1887/2012 (edited by Klaus Lichtblau).

viewed. Second, the methods and the empirical results of our study are presented. Third, we discuss our empirical findings by looking at them through different theoretical lenses. In the end, we conclude with a recapitulation of the findings and discuss some important implications as well as avenues for further research.

II. Theoretical Background and Literature Review

A) Privacy Paradox

The Internet has become an indispensable part of our lives. Growing up, studying, working, and passing one's spare time without the web is almost unthinkable for most people in industrialized countries. Social network sites (SNS) are also thriving. The biggest service, Facebook, has now more than one billion members and in Switzerland the penetration is very high, too⁵. In a conventional definition, SNS were defined as «web-based services that allow individuals to (1) construct a public or semi-public profile within a bounded system, (2) articulate a list of other users with whom they share a connection, and (3) view and traverse their list of connections and those made by others within the system»⁶.

On the web, users leave traces. To profit from the benefits of online-shopping, e-banking, social network sites, and other services they need to provide personal data. The data is collected in various ways by the providers of the services, e.g. Internet companies, such as Google and Facebook. With such data collection threats and dangers to users' privacy arise. Personal data can be abused in many ways. Sensitive data, such as credit card numbers and passwords, can be «phished». Stalking, cyberbullying, and other forms of privacy intrusion have received media attention and academic research is increasingly investigating such phenomena.

But what is privacy? WESTIN⁷ defined privacy as the «claim of individuals, groups, or institutions to determine for themselves, when, how, and to what extent information about them is communicated to others». Other authors see

⁵ SOCIAL MEDIA SCHWEIZ REPORT, Facebook – Die Schweiz in Zahlen, retrieved from http://socialmediaschweiz.ch/2013_05_31_Facebook_-_Die_Schweiz_in_Zahlen.pdf on July 10 2013).

⁶ DANAH BOYD/NICOLE ELLISON, Social Network Sites: Definition, History, and Scholarship, *Journal of Computer-Mediated Communication* 2007, 1, 210 ff.

⁷ ALAN WESTIN, *Privacy and Freedom*, 1st ed. New York 1967, 6–7.

privacy as a multidimensional – and not a one-dimensional – construct. Coming from a legal perspective, PROSSER⁸, for example, conceptualized privacy along four distinct legal torts: «1) intrusion (i.e., invading a person's solitude or seclusion), 2) appropriation (i.e., using a person's identity or image without permission), 3) disclosure (i.e., making public embarrassing private facts about a person), and 4) false light (i.e., portraying an individual in a way that inaccurately and negatively represents the person)»⁹. In sum, there exists no common definition of privacy and the exact meaning is still contended. For this article, we are interested in the information aspect of privacy and therefore apply WESTIN's definition. Thus, we are mainly concerned with point 1) of the previous enumeration.

Why do users provide so much data although they are concerned about their privacy? This question stands at the core of the so called *privacy paradox*. The privacy paradox describes the situation that Internet users are concerned about their privacy but do not act accordingly. Despite high levels of concerns users still disclose much of their very sensitive data, such as their address, phone number, location data, or political preferences. Hence, the privacy paradox describes a trade-off between attitudes and behavior in the sense that Internet users' privacy concerns are not reflected in protective behaviors. Thus, privacy concerns are not correlated with concrete actions, such as choosing restrictive privacy settings on SNS, using alternative search engines, or deleting cookies regularly¹⁰.

B) Explaining the Privacy Paradox

How can we explain – or entangle – the paradox? A first explanation is users' unawareness of the risks and problems of disclosure. In this view, they would not know about the risks of massive disclosure and the practices of data collection. In fact, YOUNG and QUAN-HAASE have shown that Internet users' *social privacy concerns* are much more pronounced than their *institutional privacy*

⁸ WILLIAM PROSSER, The Torts of Privacy, California Law Review 1960, 3, 383 ff.

⁹ CLINTON D. LANIER/AMIT SAINI, Understanding consumer privacy: A review and future directions, 1 ff., 4.

¹⁰ RALPH GROSS/ALESSANDRO ACQUISTI, Information revelation and privacy in online social networks, ACM Workshop on Privacy in the Electronic Society (WPES) 2005, 1 ff.; ZEYNEP TUFEKCI, Can You See Me Now? Audience and Disclosure Management in Online Social Network Sites, Bulletin of Science and Technology Studies 2008, 4, 544 ff.

*concerns*¹¹. Social privacy concerns describe the fear of intrusion caused by other people. They entail concerns about being stalked, easily scanned and found by employers or by unwanted acquaintances, or of being bullied and made fun of online. Thus, social privacy concerns revolve around concrete individuals. Therefore, they are accessible and easy to understand.

By contrast, institutional privacy concerns deal with companies or public institutions. Institutional privacy concerns describe people's uneasiness and fear that their data is used for unwanted purposes. Examples are unwanted, targeted ads on Facebook or political spying by the state. Compared with social privacy concerns, institutional privacy concerns are more abstract and less present in people's daily lives. Only few Facebook users in YOUNG and QUAN-HAASE's study perceived institutional privacy to be a problem, whereas social privacy concerns figured very prominently. Most respondents had very strict privacy settings – thus protecting themselves against intrusion in terms of social privacy –, but neglected the institutional aspects of privacy. While the privacy paradox is (at least partly) resolved in terms of social privacy for these users, it persists in terms of institutional privacy. Similar findings occurred in the German context, where the privacy paradox has been demonstrated for both social and institutional privacy concerns¹². Lacking knowledge about the risks of institutional privacy intrusion might be one explanation for the privacy paradox.

A second explanation would be a *rational choice approach*. The benefits of disclosing personal information on the Internet for the individual outweigh the cost or risks. This argument has seen some empirical support¹³.

Yet, it seems hardly possible for individuals to calculate the risks that are associated with disclosing data as these are contingent on a number of random factors and also depend on individual preferences. Some individuals might see targeted advertising as an intrusion into their privacy, whereas others might find it useful to get information on products they are interested in. This example demonstrates that an approach based on purely rational cost-benefit calcula-

¹¹ ALISON L. YOUNG/ANABEL QUAN-HAASE, Privacy protection strategies on Facebook: The Internet privacy paradox revisited, *Information, Communication & Society* 2013, 4, 1 f.

¹² HANNA KRASNOVA/OLIVER GÜNTHER/SARAH SPIEKERMANN/KSENIA KOROLEVA, Privacy concerns and identity in online social networks. *Identity in the Information Society* 2009, 1, 39 ff.

¹³ 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, 9, 862 ff.

tions would oversimplify the phenomenon and can therefore not lead to a substantially better understanding of the privacy paradox. Furthermore, such a cognitive rational choice approach neglects the emotional and incorporated aspects of behavior. Many actions – also online – are routinely performed or driven by irrational affective factors. We draw on this idea in the discussion of our empirical findings, when we apply the duality of *Gemeinschaft* (community) and *Gesellschaft* (society) as proposed by TÖNNIES¹⁴ to online social networks. The idea behind this is that there are some forms of social collectives that are held together by its members' internalized emotional ties and implicit rules (*Gemeinschaft*), whereas others are held together by more rational calculations and the corresponding mechanisms such as contracts and explicit legal rules (*Gesellschaft*).

Finally, *trust* is a means to resolve the privacy paradox. When people trust, they are willing to become vulnerable by relying on the other party. In our case, if users trust Internet companies or other institutions when it comes to their data, the privacy paradox would be resolved. Such an approach can be cognitive, calculative, as explained by rational choice («I trust a service because the benefits of trusting outweigh the costs») or emotional, intuitive («I trust a service because I feel it will not abuse my data or my trust»).

Conventionally, trust has been defined as «a psychological state comprising the intention to accept vulnerability based upon positive expectations of the intentions or behaviors of another»¹⁵. These positive expectations emerge from specific beliefs in terms of the transaction partner's trustworthiness¹⁶. Given the (quasi-)anonymousness of large parts of the Internet and the fact that user experiences are limited by computer-mediation, a-synchronous communication and refined impression management techniques, trust becomes all the more critical to the establishment of exchange relationships¹⁷. In fact, trust is a key prerequisite for the establishment and growth of online services¹⁸. Users need

¹⁴ TÖNNIES, (Fn. 4).

¹⁵ DENISE M. ROUSSEAU/SIM B. SITKIN/RONALD S. BURT/COLIN CAMERER, Not so different after all: A cross-discipline view of trust, *Academy of Management Review* 1998, 3, 393 ff., 395

¹⁶ D. HARRISON MCKNIGHT/VIVEK CHOUDHURY/CHARLES KACMAR, Developing and Validating Trust Measures for e-Commerce: An Integrative Typology, *Information Systems Research* 2002, 3, 334 ff.

¹⁷ YAKOV BART/VENKATESH SHANKAR/FAREENA SULTAN/GLEN L. URBAN, Are the Drivers and Role of Online Trust the Same for All Web Sites and Consumers? A Large-Scale Exploratory Empirical Study, *Journal of Marketing* 2005, 4, 133 ff.; DAVID GEFEN, E-commerce: the role of familiarity and trust, *Omega* 2000, 6, 725 ff.

¹⁸ DONNA L. HOFFMAN/THOMAS P. NOVAK/MARCOS A. PERALTA, Building Consumer Trust Online, *Communications of the ACM* 1999, 4, 80 ff.; SIRKKA L.

to perceive a sufficient level of trust to rely on the benevolence, integrity, credibility, ability and reliability of an online source¹⁹.

Users' levels of trust depend on a variety of factors. Online experience, demographic characteristics, personality traits, and the (perceived) attributes of the other party have been identified as salient drivers of trust²⁰. We expect similar dynamics to be at work, when we transfer the insights from research on e-business and online transactions to the Internet more generally. Online communities and social network sites also rely heavily on the users' experience and trust-inducing mechanisms offered by the providers. Administrators and creators of these sites must ensure that users perceive them as trustworthy – or at least trustworthy enough to engage there regularly. One approach to understand how organizations try to account for the different needs of various stakeholders and focus on value creation for society as a whole is the public value framework.

Public value refers to the contribution of any organization to the wellbeing of society. The concept originally stems from research on the strategic orientation of public sector organizations. It provides public managers with an understanding of what value their organizations create for society and enables them to manage their activities in terms of creating value for the public²¹. MOORE points out, that «managers must satisfy some kinds of desires and operate in accord with some kinds of perceptions»²². MEYNHARDT takes up this idea and links the creation of public value to the fulfillment of basic human needs²³. Drawing on value philosophy and psychological research, he arrives at four dimensions of public value:

JARVENPAA/NOAM TRACTINSKY/MICHAEL VITALE, Consumer Trust in an Internet Store, *Information Technology and Management* 2000, 1–2, 45 ff.; MING ZHOU/DING TIAN, An Integrated Model of Influential Antecedents of Online Shopping Initial Trust: Empirical Evidence in a Low-Trust Environment, *Journal of Informational Consumer Marketing* 2010, 2, 147 ff.

¹⁹ ANOL BHATTACHARJEE, Individual trust in online firms: Scale development and initial test, *Journal of Management Information Systems* 2002, 1, 211 ff.

²⁰ For a more comprehensive overview, see: CHRISTOPH LUTZ/CHRISTIAN P. HOFFMANN/ANDREA VON KAENEL, Perception is Reality – The Impact of Buyer and Seller Attributes on Online Trust, in: Jens Vollmar/Roman Becker/Isabella Hoffend (eds.), *Macht des Vertrauens*, Berlin/Heidelberg 2013, 185 ff.

²¹ MARK H. MOORE, *Creating Public Value – Strategic Management in Government*, 1st ed., 1995 Cambridge (MA).

²² MOORE (Fn. 21), 52.

²³ MEYNHARDT (Fn. 3), 192 ff.

- A *moral-ethical* component can be derived from a basic need for a positive self-evaluation.
- The basic need of maximizing pleasure and avoiding pain translates into a *hedonistic-aesthetical* dimension.
- There is a basic need for gaining control and coherence over one's conceptual system and environment. This is reflected in the *utilitarian-instrumental* dimension of public value.
- Finally, individuals want to feel as part of a group and have positive relationships with others. This is the basis for a *political-social* dimension of public value.²⁴

Importantly, MEYNHARDT²⁵ makes clear that public value is only created, respectively destroyed, when individuals perceive their relationship to the public positively or negatively influenced. Therefore, public value creation is never only about «objective» facts, but needs to be reflected in people's perceptions and subjective evaluations.

Public value is, however, not limited to public administration. All kinds of organizations influence societal values and are evaluated based on their public value creation: «one cannot but influence public values»²⁶. GRANOVETTER teaches us that economic activities are always embedded in a social context²⁷. Therefore, we find it promising to employ the public value approach when evaluating issues of organization's privacy protection and data security.

Based on public value theory, a Swiss initiative of business leaders, politicians and academics, the «Swiss Dialogue» has issued a declaration on *Responsibility and Informational Self-Determination on the Internet*²⁸. In that document, they postulate that organizations make sure that data cannot be used for harmful purposes and enable users to decide themselves how their data is used. The Internet provides ample opportunities for innovative business models with a high potential for public value creation, which should be used accordingly. Also, informational self-determination is a condition for sustainable business-

²⁴ MEYNHARDT (Fn. 3), 203.

²⁵ TIMO MEYNHARDT, Public Value – oder: was heisst Wertschöpfung zum Gemeinwohl? dms – der moderne staat 2008, 2, 457 ff.

²⁶ MEYNHARDT (Fn. 3), 193 (emphasis in original).

²⁷ MARK GRANOVETTER, Economic Action and Social Structure. The Problem of Embeddedness, American Journal of Sociology 1985, 3, 481 ff.

²⁸ www.schweizerdialog.ch; see TIMO MEYNHARDT/PETER GOMEZ, The Pyramid of Business Responsibilities: An Alternative to Carroll's Approach. Journal tbd 2013, forthcoming article for a theoretical account.

models that create profits for companies and material wealth for society. Finally, not every behavior can be anticipated and regulated by law, especially on the Internet which is subjected to technological change on an ongoing basis. Therefore, decision-makers need to think about the consequences of their actions and act responsibly beyond mere legal compliance. This might include, for example, voluntary commitments on how to deal with the data entrusted to them.

III. Methods and Results

A) Data and Sample

We use survey data from Switzerland. In order to ensure a sample representative of the overall population, the survey was conducted by telephone. A leading international market research institute provided both access to a representative sample and the execution of the interviews. Interviews were conducted in May 2012, involving a sample of 1002 respondents. Of those, 53 percent are male and 47 percent female. About 35 percent have a high level of education, almost 60 percent a medium level, and about 5 percent have low levels of education. As for the age distribution, respondents aged 30–49 represent the largest group in the sample (45 percent), followed by 15–29 year olds (28 percent), and 50–74 year olds (27 percent).

The questionnaire covered eleven constructs and single items regarding privacy and security attitudes as well as electronic identity and serendipity, seven of which were also part of a Eurobarometer survey²⁹.

For the descriptive analysis of the data we used SPSS Statistics (Version 20). A more comprehensive overview of the data can be found in HOFFMANN et al.³⁰.

²⁹ The Special Eurobarometer 359 «Attitudes on Data Protection and Electronic Identity in the European Union» was published in June 2011 and the fieldwork lasted from November 2010 to December 2010. The topics of the survey cover privacy, identity management and data protection. In total, 26574 Europeans from all the 27 EU member states were interviewed. For the whole report, see:
http://ec.europa.eu/public_opinion/archives/ebs/ebs_359_en.pdf

³⁰ CHRISTIAN HOFFMANN/CHRISTOPH LUTZ/MIRIAM MECKEL/GIULIA RANZINI, An Element of Surprise: The Impact of Serendipity on Online Trust, Academy of Management Annual Meeting 2013 (Orlando, FL), 1 ff.

B) Descriptive Part

Respondents generally exhibit low levels of *trust* in Internet companies and telecommunication providers (see table 1).

On the other hand, government agencies enjoy high levels of trust: 85 percent of respondents think they can trust or totally trust the government when it comes to the protection of personal data. Also financial institutions and medical service providers (e.g. hospitals) are generally perceived as trustworthy – although a little bit less than the government. Still only about 20 percent of the population does not trust these institutions. In the middle, we find European institutions, where about half of the respondents trust, while the other half does not trust.

	<i>Internet (T1)</i>	<i>Companies</i>	<i>Telecommunication Providers (T2)</i>
Totally trust	0.3 (3)		2.2 (22)
Tend to trust	13.8 (138)		23.7 (237)
Tend not to trust	45.7 (458)		44.4 (4459)
Do not trust at all	38.1 (382)		28.0 (281)
Do not know	2.1 (21)		1.7 (17)
Total	100 (1002)		100 (1002)

Table 1: Trust in Internet companies and telecommunication providers

Comparing these values with other countries in Europe, Swiss people are more skeptical and less trusting towards Internet companies as well as telcos than the European average. In the EU27 22 percent of the population trust Internet companies and 32 percent trust telcos (Eurobarometer). Interestingly, there is a considerable difference in «Do not know» between the Swiss sample (about 2 percent) and the EU27 average (16 percent for Internet companies but only 5 percent for telcos). Swiss people's trust levels in government are among the highest in Europe, closely resembling the states in Northern Europe (Denmark, Finland, Sweden, Estonia).

Regarding *privacy concerns*, about half of the users are concerned about the use of their data for direct marketing/junk ads, while the other half is not. About 10 percent are very concerned and only about 3 percent are not concerned at all. This is in line with general tendencies in Europe. Here, about 70 percent are concerned about companies using their personal information in undesired ways.

Finally, users take different *measures to protect their privacy* online: deleting the browser history and cookies are the most common forms. A vast majority indicates that they delete the search history and cookies at least sometimes. However, only a small minority uses alternative or encrypted search engines that do not personalize people's web search.

C) Explanatory Part

Do users' privacy concerns lead to more protective behavior? Do users' levels of trust in Internet companies and telcos lead to more protective behavior? Or is there a trade-off between attitudes and behavior, as described by the privacy paradox?

To answer these questions, we correlate users' privacy concerns (measured by the variable «I am concerned about the use of my personal data for direct marketing and targeted ads») with their privacy protection behavior, as expressed by a summed-up index of eight statements³¹ (e.g. «I delete my browser history», «I use alternative search engines», or «I delete my cookies»). The Pearson's correlation between privacy concerns and effective behavior is rather low and has a value of -0.14. However, the correlation is strongly significant and negative. Thus, the privacy paradox does not turn out to be present in our data. Or in other words, people who worry more about the protection of personal data are more cautious on the web. They apply more measures to protect themselves compared with the less concerned counterparts.

When we look at the single correlations between privacy concerns and protection behavior (instead of the summed-up index), only one effect is insignificant: «Using location-based services» – such as Foursquare. Here, we find no significant correlation between privacy concerns and behavior. Thus, users with high privacy concerns use location-based services equally often as the unconcerned. Given that location-based information is especially private and sensitive, encountering the paradox in this strong case (compared to other more «symbolic» measures, such as «deleting cookies» or «deleting the search history from the browser») indicates that also in Switzerland there might be a divergence between attitudes and behavior when it comes to online privacy. However, the trade-off is stronger for «new» and lesser known forms of Internet use, such as location-based services. In fact, the large numbers of people unfamiliar with such applications (about 25 percent «do not know»; and the

³¹ The items that build the index were measured with 5-point Likert scales (never (1) – rarely (2) – sometimes (3) – often (4) – very often (5)). Thus, the maximum value of the index is 40 (8*5) and the minimum value is 8 (8*1).

effective number might even be higher due to social desirability) points to a certain insecurity towards these techniques. Knowledge seems to be a key factor in explaining the paradox.

In a second step, we controlled for demographic characteristics of the users. Table 2 shows the regression results.

		Unstandardized Coefficient	Standardized Coefficient	Sig.
<i>Privacy Concerns</i>		-1.38	-.17	.00
<i>Region</i>		.12	n. s.	n. s.
<i>Countryside vs. City</i>		.74	n. s.	n. s.
<i>Gender</i>		-.95	-.08	.04
<i>Age</i>		.68	.08	.04
<i>Education</i>		-.20	n. s.	n. s.
<i>Employment Status</i>		.13	n. s.	n. s.
<i>Household Size</i>		-.49	n. s.	n. s.
<i>Home ownership</i>		-.25	n. s.	n. s.
<i>Life Stage Segmentation</i>		-.11	n. s.	n. s.
<i>Household Income</i>		.25	.08	.03

R² = 0.05; S. E. = Standard Error; Sig. = Significance Level

Table 2: Linear regression of privacy protection behavior Index on privacy concerns and control variables

The overall influence of privacy concerns on the protection behavior index remains significant and negative. Thus, the higher Swiss people's privacy concerns, the more protective behavior they reveal. Again, the privacy paradox seems to be less pronounced than in other contexts. Next to privacy concerns, certain demographic characteristics explain users' protective behavior. Men are generally more protective than women (the gender variable is coded «1 – Man; 2 – Woman»). However, the absolute effect is not very strong, as the difference

between men and women is only 1 point on a scale with range 32. The age effect indicates that older users are more protective than younger ones. Unfortunately, we do not have information about the time spent online and the forms of using the Internet. Thus, the age effect might well be caused by different behavior of elderly people on the web compared with younger ones. Finally, income is a significant predictor of the dependent variable. Higher salaries lead to more cautious behavior. This is not surprising, because for people with higher income, there is more at stake on the Internet, and they have more to lose.

We also ran the same regression model with the two *trust* items (trust in Internet companies and trust in telcos) as additional independent variables. Neither of the two trust items turned out to be significantly associated with protective behavior. Thus, the privacy paradox is much more prevalent for the institutional aspects (trust) than the more social aspects (privacy concerns). The very low and insignificant correlations of 0.03 (Internet companies) and 0.05 (telcos) between trust and protection behavior point in the same direction. They underline the fact that distrusting individuals are not more careful online than trusting ones. The absence of the effect is partly attributable to the skewed distribution of the trust variables, i.e. the very low levels of Swiss people's trust in Internet companies and telcos (Table 1). Still, positive and significant correlations between trust and privacy concerns (of 0.15) indicate that distrust in Internet companies and telcos does in fact capture people's concerns. Therefore, the story of the trust paradox conveys a version of the privacy paradox that is less obvious and direct than the usual version. It addresses the more subtle and institutional facets of online privacy and behavior.

IV. Discussion

First, comparing the levels of trust between different sectors and industries it emerges as interesting that financial institutions enjoy fairly high levels of trust concerning their dealing with data. At the same time, indicative studies have shown that their public value is relatively low. This appears surprising at first sight. However, «public value (...) is the combined view of the public about what they regard as valuable»³². The privacy paradox points in a similar direction: if people do not alter their behavior when they suspect violations of privacy, privacy protection seems not to be particularly valuable to them. At the

³² COLIN TALBOT, Paradoxes and prospects of «public value». *Public Money & Management* 2011, 1, 27 ff., 28.

same time, the data indicates that if an organization handles data appropriately, this does by no means imply a high public value. Here, the declaration of the «Swiss Dialogue» seems to provide a viable pathway: data protection as such does not constitute a public value, unless it is valued by the public. The public value approach explicitly acknowledges changing value dynamics in society and therefore opposes the attribution of absolute values to certain constructs. Nevertheless, users that value their privacy should be able to protect their data following the principle of informational self-determination. Condemning all forms of data collection seems misleading as the Internet and the relatively recent big data and open data movements offer ample opportunities for innovative business models that might create public value³³.

Second, the distinction between *social* and *institutional* privacy concerns warrants some attention. In the end, most forms of privacy protection behavior, such as privacy settings on SNS, can help users alleviate concerns about social privacy, but do not solve institutional privacy concerns, as the data is still used by companies to target advertising and we can also not assume that privacy settings will stop secret services from using data that is entered on SNS. Hence, the fact that SNS are widely used, whereas users have institutional privacy concerns shows that the privacy paradox persists.

We think that the differentiation between *social* and *institutional* privacy concerns on SNS and the different attitudes of users towards these two components can partly be explained by a very basic sociological concept, namely the duality of *Gemeinschaft* (community) and *Gesellschaft* (society) as proposed by FERDINAND TÖNNIES³⁴ (1887/2012)³⁵. *Gemeinschaft* refers to traditional forms of social collectives that are held together by implicit rules of behavior, their member's emotional ties and embedded rituals. Examples of such collectives include families or groups of friends. On the other hand, *Gesellschaft* is characterized by a rationalization of the social collective that arises from exchange relationships. The motive for being part of a social collective shifts from organic emotional attachment (*Wesenswille*) to a rational consideration where other individuals and being part of a collective are seen as means to an

³³ DAVID BOLLIER, *The Promise and Peril of Big Data*, 1st ed., Washington DC 2010; DELOITTE LLP, *Open Data: Driving growth, ingenuity and innovation*, London 2012; VIKTOR MAYER SCHÖNBERGER/KENNETH CUKIER, *Big Data: A Revolution That Will Transform How We Live, Work and Think*, 1st ed., London 2013..

³⁴ TÖNNIES, (Fn. 4).

³⁵ This application of TÖNNIES is mainly useful for more social aspects of the Internet, i.e. for SNS, blogs, online communities, and other forms of social media. It might not be as applicable and accurate for other uses of the Internet, where privacy is also an issue, for example online search, e-banking, and online shopping.

end (*Kürwille*)³⁶. Therefore, *Gesellschaft* relies on explicit, codified rules and contracts between its members. In a way, *Gemeinschaft* is closer to the individual as it stems from «warm» feelings, instinct and shared experiences, whereas the more abstract and rational *Gesellschaft* initially is something strange, that is based on «cold» analytic rationalizing and cost-benefit calculations.

The use of SNS represents a form of post-traditional community building³⁷. And indeed there seem to be some parallels with TÖNNIES' characterization of *Gemeinschaft*: rules of behavior in online social networks are mostly implicit and individuals foster their relationships and search for a feeling of belonging. In such *Gemeinschaft*-like forms of social collectives users are willing to provide information and data about themselves as this is an implicit part of being a member of the community.

By contrast, the dangers associated with institutional privacy concerns are very abstract. Even if users know on an abstract level that their data is used for commercial purposes and might be accessible for secret services, these dangers seem very strange and do not correspond to actual feelings of being threatened. This might explain why user's institutional privacy concerns are less pronounced³⁸. One could idealize this as a situation where the emotional attraction of being part of an online community (*Gemeinschaft*) trumps the abstract danger of data misuse (*Gesellschaft*). If we take TÖNNIES' duality of *Gemeinschaft* and *Gesellschaft* into account and thereby acknowledge that individual behavior is not purely the result of rational choice, the privacy paradox seems to be partly resolved.

Thirdly, the data indicates that younger users are less protective than older ones. This might be explained by a larger amount of time spent online or different forms of using the Internet, two variables we could not control for. However, it might also point to a generational cleavage concerning the attitude to-

³⁶ TIMO MEYNHARDT, Management zwischen Main Street und Wall Street, in: Sascha Spoun/Timo Meynhardt (eds.): Management – eine gesellschaftliche Aufgabe. Baden-Baden, 19 ff.

³⁷ RONALD HITZLER, Brutstätten posttraditionaler Vergemeinschaftung, in: Ronald Hitzler/Anne Honer/Michaela Pfadenhauer (eds.): Posttraditionale Gemeinschaften. Theoretische und ethnografische Erkundungen, Wiesbaden 2008, 55 ff.; SEBASTIAN DETERDING, Virtual Communities. in: Ronald Hitzler/Anne Honer/Michaela Pfadenhauer (eds.): Posttraditionale Gemeinschaften. Theoretische und ethnografische Erkundungen, Wiesbaden 2008, 115 ff.

³⁸ ALISON L. YOUNG/ANABEL QUAN-HAASE, Privacy protection strategies on Facebook: The Internet privacy paradox revisited, Information, Communication & Society 2013, 4, 1 ff.

wards privacy. After all, privacy is not absolute, but a socially defined construct, that is subject to change. Younger generations are more used to provide their own data and find personal data about others online. This might change attitudes towards privacy. Such interpretation poses a challenge to political positions and often heard statements that a certain level of privacy has to be protected as these claims might oversee that the construct itself is in a state of flux.

What is the role of trust in resolving the privacy paradox? Trust can help to resolve the paradox from two different angles: the attitudinal side of the equation (concerns) and the behavioral side (protection behavior, disclosure). Trust concerns both the supply-side (Internet companies, telcos) and the demand-side (users) of the equation. Table 3 contains an idealized matrix of how different solutions align behavior and attitudes so as to overcome the privacy paradox and brings trust back into play.

	Organization (Internet companies)	Users
Concerns	Engaging in dialogue with users; Fostering trust via transparency and accessibility; Self-binding industry-wide mutual agreements; International legislation	Building knowledge; Discussing issue(s) with friends and experts; Socialization; Education; Trusting the trustworthy services
Behavior	Providing users with easy-to-use and understandable protection options; Trusting in users' ability and willingness to make use of these possibilities; Specific solutions for specific groups (e.g. elderly, adolescents etc.); Contextual privacy practices to foster context-specific trust	Making use of protection possibilities, Disclose less; Trusting the technical solutions; Informational self-determinism; Principle-driven approach to using the web

Table 3: Different ways to resolve the privacy paradox with a special focus on trust

It shows that privacy on the Internet is a multi-faceted and multi-contextual issue, where several stakeholders are involved. Users and the providers are the most important ones, but other institutions also have their role. Schools, universities and other educational institutions can enhance people's knowledge and alleviate fears as well as myths about online privacy. Families can include

the topic in their daily conversations. Politicians of different parties should also put the topic up on their agendas.

Understanding how institutions can sensitize individuals about their trust and behavior is an important step in appeasing the current tensions between big-Internet companies on the one hand and concerned users on the other hand. NISSENBAUM's concept of contextual privacy provides a useful framework to guide such understanding³⁹. It brings context back into play and argues that Internet companies should ask users for permission to use their data depending on the informational and privacy norms at play – but not on a catch-it-all basis. This is also in line with the aforementioned declaration of the Swiss Dialogue about informational self-determination and public value creation. Existing off-line privacy practices, e.g. in the financial or medical sector, could inform the development of sensible online privacy frameworks.

V. Conclusion

This contribution started with the observation that online our privacy is increasingly undermined, be it through secret services' spying or commercial use of our data. We describe how people are concerned about such practices whereas their concerns stand in stark contrast with the frequent use of search engines, SNS and other online services, where they generously and voluntarily provide personal data.

This privacy paradox could be partly confirmed with survey data from Switzerland. Interestingly, the data suggests a differentiation between institutional and social privacy concerns. Also, there are major differences between institutions when it comes to trust in data protection: banks and the government enjoy relatively high levels of trust, whereas Internet companies and providers are not trusted.

We have discussed the empirical results through a number of different theoretical lenses:

First of all, the public value approach was used to explain why organizations that enjoy high levels of trust concerning data protection are not automatically seen as especially valuable to society. The value relativist nature of the public value approach calls for a differentiated view on big data and privacy: users

³⁹ HELEN NISSENBAUM, A Contextual Approach to Privacy Online, *Daedalus* 2011, 4, 32 ff.

should be able to tailor privacy settings to their needs in the sense of informational self-determination, but from a societal perspective we should also take into account the opportunities for public value creation that arise from big data and the Internet in general. Such a relativist view on the value of privacy seems especially appropriate when we take changing attitudes and social conventions about privacy into account.

Second, the distinction between community and society that goes back to the work of FERDINAND TÖNNIES could partly resolve the privacy paradox. SNS constitute a modern form of community building that speaks to users' emotional needs for social belonging (*Gemeinschaft*). Yet, the risks associated with the abuse of data are very abstract and might be comprehended on a rational level but do not translate into an actual feeling of fear (*Gesellschaft*). In this case, the urge of being member of a community seems to trump the abstract recognition of data security issues.

Third, the data indicates that younger users are less concerned about the abuse of their data. This points to an understanding of privacy not as an absolute right to be protected at any price but as a socially defined construct that is subject to societal processes of negotiation and change over time. This interpretation fits well with the public value view, where privacy as such is not ascribed a public value and where value is always the result of positive evaluations reflected in people's perception.

Fourth, trust proves as a useful lens to discuss online privacy, especially the institutional aspects. The privacy paradox turned out to be a trust paradox in our case. Although Swiss people reveal very low levels of trust in Internet companies and telcos, they do not rely heavily on privacy protective behavior. Or in more technical terms, there is no connection between trust and effective (self-reported) behavior. Why then, one might ask, bother to increase the trust levels? First of all, a climate of distrust is not a very satisfying situation on the long run and large scale studies have shown that trust and social capital have an economic impact⁴⁰. So, more trust might be better for the economy. Second, we demonstrated that trust is not an isolated construct and functions in conjunction with people's (privacy) attitudes and behaviors. We presented four avenues to overcome the privacy paradox by focusing on users and Internet companies. Different institutions and stakeholders must work together to improve the current situation.

At the same time, we must differentiate between different contexts as privacy is very much a contextual phenomenon. Whereas users might be concerned to

⁴⁰ STEPHEN KNACK/PHILIP KEEFER, Does Social Capital Have an Economic Payoff? A Cross-Country Investigation, *Quarterly Journal of Economics* 1997, 4, 1251 ff.

leave their phone number in one setting, e.g. in the comment section of an online newspaper, they might be readily willing to do so in another one, e.g. in a closed and encrypted e-banking environment. Furthermore, online trust can and should be further differentiated into distinct dimensions, as many studies in the information systems context have shown⁴¹.

One limitation, therefore lies in the broad and generalized concept of trust and privacy used in the questionnaire. Qualitative research should explore the connections of trust, privacy concerns, behavior, and the role of the different institutions and organizations involved in specific contexts (e.g. in e-banking, online discussion boards or in the use of VoIP, such as Skype).

Further research could concentrate on the public value creation by innovations, be it in business, the public or the nonprofit sector, which are enabled by big data and a corresponding decline in user's privacy. Such a research program could start with in-depth case studies in order to inquire which aspects of big data are publicly accepted, adding value along the four public value dimensions, and which ones are not seen as legitimate. Additionally, further empirical work could concentrate on the question whether there really is a shift in privacy attitudes over time and how the variables trust, public value and privacy behavior relate to each other.

⁴¹ McKNIGHT/CHOUDHURY/KACMAR (Fn. 16), 334 ff.