JOURNAL OF PSYCHOSOCIAL RESEARCH ON CYBERSPACE
CYBERPSYCHOLOGY

Hoffmann, C. P., Lutz, C., & Ranzini, G. (2016). Privacy cynicism: A new approach to the privacy paradox. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace, 10*(4), article 7. doi: 10.5817/CP2016-4-7

Privacy cynicism: A new approach to the privacy paradox

Christian Pieter Hoffmann[1], Christoph Lutz[2], Giulia Ranzini[3]

[1] University of Leipzig, Leipzig, Germany
[2] BI Norwegian Business School, Oslo, Norway
[3] VU University Amsterdam, Amsterdam, The Netherlands

Abstract

Privacy concerns among Internet users are consistently found to be high. At the same time, these concerns do not appear to generate a corresponding wave of privacy protection behavior. A number of studies have addressed the apparent divergence between users' privacy concerns and behavior, with results varying according to context. Previous research has examined user trust, lack of risk awareness and the privacy calculus as potential solutions to the "privacy paradox". Complementing these perspectives, we propose that some users faced with seemingly overwhelming privacy threats develop an attitude of "privacy cynicism", leading to a resigned neglect of protection behavior. Privacy cynicism serves as a cognitive coping mechanism, allowing users to rationalize taking advantage of online services despite serious privacy concerns. We conduct an interdisciplinary literature review to define the core concept, then empirically substantiate it based on qualitative data collected among German Internet users.

Keywords: Online privacy; institutional privacy concerns; privacy cynicism; scale development; focus groups

Introduction

Recent revelations, such as Edward Snowden's release of secret information on the PRISM program, have led many Internet users to question their ability to effectively control the spread and use of personal data on the Internet (PEW Research, 2014). According to public perception, intelligence agencies – supported by large Internet service providers – are able to collect and analyze sensitive information about citizens to an unprecedented degree. As a result, Internet users express significant privacy concerns.

At the same time, a number of studies have found that Internet users only sparingly engage in privacy protection behavior, e.g., by restricting online privacy settings or deleting cookies – an apparent discrepancy between attitudes and actual behavior that has led some to declare a "privacy paradox" (Acquisti, 2004; Lanier & Saini, 2008). In fact, such a discrepancy would seem to oppose established behavioral theories such as the theory of planned behavior (Ajzen, 1991). Consequently, numerous studies have explored the relationship between privacy attitudes and behavior, finding only a weak, if any, effect, depending on the research context and methodology applied (see Kokolakis, 2017 for a review).

A more recent differentiation finds that the evidence for the existence of a "privacy paradox" is strongest when it comes to institutional privacy threats (Raynes-Goldie, 2010; Young & Quan-Haase, 2013). In other words, users do tend to adapt to privacy threats emanating from their immediate social environment, such as stalking and cyberbullying, but react less consistently to perceived threats from institutional data retention (boyd & Hargittai,

2010). As a result, commercial service providers criticized for their privacy policies, such as Google, Facebook or Apple, still dominate consumer markets, while less privacy-intrusive services, such as TOR or alternative search engines, fail to reach significant market penetration.

In this paper, we will address previous studies framing the "privacy paradox" as a divergence between attitudes and behavior related to (online) privacy (Barnes, 2006; Tufekci, 2008). We will review theoretical perspectives applied to the phenomenon and develop a complementary explanation. By introducing the concept of "privacy cynicism", we will strengthen the argument that, even when it comes to institutional privacy threats, users' attitudes and behavior do not diverge. Rather, users develop attitudes to cope with the specific challenges of institutional privacy threats. More specifically, we will argue that some users develop attitudes of privacy cynicism, in order to avoid cognitive dissonance (Festinger, 1957). We define privacy cynicism as an *attitude of uncertainty, powerlessness and mistrust towards the handling of personal data by online services, rendering privacy protection behavior subjectively futile*.

We will describe Internet users' development of privacy cynicism attitudes as a coping mechanism, allowing for the rationalization of apparent disparities between subjective concerns and observable behavior. Thereby, the consideration of privacy cynicism attitudes complements previous explanations for apparent paradoxes in the context of institutional privacy threats. The paper will develop the privacy cynicism concept based on a literature review and illustrate it based on qualitative data collected in focus groups with German Internet users in late 2014.

Theoretical Background

Privacy concerns and behavior. The question as to 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 Susan Barnes (2006) to define the perplexing divide between privacy-concerned adults and self-disclosing digital teenagers, has evolved to incorporate discrepancies between individual attitudes and behavior when it comes to (online) privacy (Tufekci, 2008). A number of studies have found privacy concerns (attitude) to exert only a weak, if any, effect on online self-disclosure or protection behavior (behavior) (Dienlin & Trepte, 2015; Kokolakis, 2017).

In order to explain this "privacy paradox", scholars have developed several interpretations as to why individuals would disclose private information despite pronounced privacy concerns. Lee, Park and Kim (2013) have grounded their approach on the concept of a **privacy calculus**, i.e. a rational decision individuals take about disclosing personal information on the Internet when weighing benefits against costs and potential risks. Under this approach, the decision to disclose information relies heavily on individual sensitivities towards what is perceived as privacy invasive (Hurwitz, 2013). The privacy calculus explanation is also heavily contingent upon users' level of awareness and understanding of the benefits and risks associated with any online action, or transaction.

A second theoretical approach to explaining online self-disclosure despite privacy concerns focuses on **user trust**, i.e. "a psychological state comprising the intention to accept vulnerability based upon positive expectations of the intentions or behaviors of another" (Rousseu, Sitkin, Burt, & Camerer, 1998, p. 395). In this view, users do not necessarily consider and evaluate the specific risks and benefits of an online transaction. Rather, they form generalized expectations towards transaction partners (Bhattacharjee, 2002; McKnight, Choudhury, & Kacmar, 2002), akin to a heuristic, allowing for a more carefree reliance on the trustee. This approach complements the privacy calculus-perspective by considering both cognitive and affective motives for online self-disclosure (Krasnova, Spiekermann, Koroleva, & Hildebrand, 2010). Nonetheless, while trust represents a key prerequisite for the establishment and growth of online services (Hoffman, Novak, & Peralta, 1999; Jarvenpaa, Tractinsky, & Vitale, 2000), there is little evidence indicating that users actually trust those services they disclose personal information on or to, such as social network sites (SNS; Klara, 2016; Young & Quan-Haase, 2013).

A third explanation for why individuals disclose personal information despite pronounced privacy concerns is to be found in their **lack of risk-awareness** and missing knowledge related to the potential harm associated with

online self-disclosure. According to this view, many users simply lack understanding and awareness of online privacy risks (Bartsch & Dienlin, 2016; Hoofnagle, King, Li, & Turow, 2010; Trepte et al., 2015). Such a lack of understanding and awareness may be due to users' digital skills, or lack thereof (Dienlin & Trepte, 2015; Park, 2013). The sociological literature on online skills suggests that privacy behavior and digital literacy or skills are related. For example, boyd and Hargittai (2010) conducted a longitudinal survey with more than 1000 first-year students (mostly 18 or 19 years old) at the University of Illinois Chicago. They found that within one year, these students became more aware of the Facebook privacy settings and modified them more often, indicating learning effects. The authors showed that highly skilled Facebook users modified their privacy settings more frequently than less skilled users.

In a subsequent study, Hargittai and Litt (2013) looked at young users' privacy behavior in the job search context, finding "that women, Whites, and those with higher Internet privacy skills are more likely to manage self-presentation online actively" (p. 43). Park (2013) came to similar conclusions and found a positive effect of three literacy dimensions (technical familiarity, surveillance awareness and policy awareness) on privacy protection behavior. Thus, general Internet skills and, more specifically, privacy skills or literacy might be a better predictor of privacy behavior than privacy concerns. Yet, a recent study on privacy literacy (Bartsch & Dienlin, 2016) reveals that most users' privacy literacy is low (with little variance in privacy literacy) and that its effect on (social) privacy behavior is weak.

Some scholars have pointed out that current Internet applications, such as SNS, are associated with a puzzling variety of privacy threats, such as social, psychological or informational threats (Dienlin & Trepte, 2015), growing ever more challenging for users to navigate. Young and Quan-Haase (2013) have shown that users' social privacy concerns are more pronounced than their institutional privacy concerns. Accordingly, users more readily adapt their protection behavior to social than institutional privacy concerns. As social privacy concerns revolve around user behavior, they may be more accessible and easy to understand for users, again highlighting the importance of awareness and understanding. Similar results have been found in the German context, where the privacy paradox has been demonstrated for both social and institutional privacy concerns (Krasnova, Veltri, & Günther, 2012).

To summarize, while the privacy paradox has been confirmed in a range of studies, some examinations did find a significant albeit weak effect of privacy concerns on online behavior (Kokolakis, 2017). Thus, the empirical evidence on the "privacy paradox" is as mixed as the theoretical perspectives applied are varied. According to Kokolakis (2017), who carried out a systematic review of the privacy paradox literature and considered 51 articles, more studies find evidence for the paradox than not. However, with more and more intervening variables being taken into consideration, the evidence for a pronounced paradox appears to be weakening over time. As the wealth of data and theoretical perspectives applied to privacy concerns and behavior expands, the "privacy paradox" may ultimately disappear (cf., Dienlin & Tepte, 2015).

To further contribute to our understanding of discrepancies between reported privacy concerns and protection behavior, this study will put forward a new concept, complementing the approaches outlined above: privacy cynicism. We argue that limitations to users' Internet literacy and skills prevent numerous users from carefully weighing the benefits of an online transaction against its potential costs (privacy calculus). While user trust could explain why institutional privacy risks are discounted by users, there is little evidence for a sufficient level of trust in data-intensive online services, such as SNS. In fact, the questionable reputation of large Internet services, such as Facebook or Google, would imply widespread mistrust and institutional privacy concerns (Klara, 2016). Persistently high levels of online privacy concerns also limit the explanatory power of lacking risk awareness for the "privacy paradox".

In summary, users' lack of privacy protection behavior as well as persistent and widespread online self-disclosure despite high levels of institutional privacy concerns remains a phenomenon in need of theoretical scrutiny. In the next segment, we will propose privacy cynicism as a new, complementary explanation for the "privacy paradox", incorporating some of the arguments put forth above.

Privacy cynicism. Users trying to weigh the benefits of online transactions against their potential costs but lacking the ability to fully grasp institutional privacy risks could be expected to refrain from online self-disclosure

and/or engage in protection behavior. After all, a lack of Internet skills or literacy would render extensive protection behavior too cumbersome, but at the same time would also increase the subjective risk associated with online transactions – and thereby aggravate privacy concerns. Interestingly, a recent study by Dienlin and Metzger (2016) reveals that Facebook self-efficacy is associated with higher self-withdrawal from the platform. Thereby, high-skilled users react to privacy concerns by applying avoidance strategies. At the same time, the study shows that perceived benefits are a strong driver of online self-disclosure. So what can (low-skilled) users do, if trapped between unclear and unmanageable privacy risks on the one hand and the promise of tantalizing service benefits on the other hand? How can transactions be carried out in agreement with assumed but barely understood risks and the associated concerns? Would engaging in risky online transactions despite risk awareness not result in cognitive dissonance (Festinger, 1957)?

We propose that the concept of cynicism, applied to privacy, might help in our understanding why individuals make extensive use of online services while avoiding privacy protection behavior despite significant privacy concerns and, in many cases, despite a lack of Internet skills. More specifically, we propose that *privacy cynicism* represents a cognitive coping mechanism for users, allowing them to overcome or ignore privacy concerns and engage in online transactions (and self-disclosure) without ramping up privacy protection efforts.

Similar to the trust construct, cynicism has been explored primarily in dyadic relationships – cynicism is typically directed towards a significant other, an interaction partner. A frequently cited element of cynicism is the speculation or intuition on the interaction partner's motives (Mills & Keil, 2005). Generally, cynicism entails the assumption that the interaction partner is motivated by self-interests divergent from one's own. Therefore, the interaction partner might try to take advantage of or mislead the person concerned. As the trust concept is based on an assumption of competence, benevolence and integrity (Bhattacharjee, 2002; McKnight et al., 2002), cynicism implies a certain level of mistrust, even antagonism (Almada et al., 1991).

Cynicism is typically associated with both uncertainty and limited power or even powerlessness: First, the person concerned has to be unsure about the other's motives in order to resort to cynicism. For example, if the hostility of the other party is a known fact, it would not be cynical to mistrust or question his/her actions or statements. Second, if the person concerned could fully control the interaction partner, he or she would not need to be concerned about its motives and actions (i.e., would not need to resort to cynicism).

Cynicism has been studied in a number of contexts besides psychology (Smith & Pope, 1990). One field of application is organization studies and human relations research, focusing on employee cynicism towards employers (Dean, Brandes, & Dharwadkar, 1998). Organizational change and restructuring efforts have been shown to be especially prone to employee cynicism, as employees are largely dependent upon their employer, vulnerable to opportunistic behavior and uncertain or skeptical about employer motives and rhetoric. Workplace cynicism has been linked to burnout, specifically in the context of social work (Salanova, Llorens, Garcia-Renedo, Burriel, & Bresc, 2005). Other studies have focused on a particular occupational context, such as a slew of studies on "police cynicism" displayed towards both the organization/employer, the efficacy of the task and institutions (such as the law) (cf., Langworthy, 1987; Regoli, 1976). In communication research, a number of studies have focused on citizen cynicism towards political institutions or the media (cf. Cappella & Jamieson, 1996; Valentino, Beckmann, & Buhr, 2001). Depending on context and application, cynicism has been defined as a trait, an attitude (general or specific) or a belief (Andersson, 1996; Dean et al., 1998).

In all of the mentioned research contexts, cynicism has been shown to function as a coping mechanism in adverse circumstances – such as doing a job or fulfilling a role despite uncertainty, powerlessness and mistrust. Working as a reactive force, and stemming from pessimistic expectations of other individuals, authority or society at large, cynicism invokes a level of resignation that allows individuals to discount risks or concerns without ignoring them (Kanter & Mirvis, 1989). Similar to trust, cynicism lets individuals face uncertainty and take on risk, but not due to favorable estimations of the significant other, quite the opposite. By acknowledging a lack of power over the situation, individuals do not discount the risk inherent in an interaction, but ascribe the responsibility for possible (or even likely) harm to forces outside of individual control. Inaction in the face of risk, thereby, becomes a rationally as well as affectively defensible choice. We propose that the concept of cynicism can be applied to online self-disclosure and institutional privacy threats, in particular. Despite corporate rhetoric, user trust in large online service providers is quite limited (Lutz & Strathoff, 2013). High levels of privacy

concerns indicate mistrust and skepticism towards the integrity and benevolence of online services. At the same time, users – low-skilled users in particular – have very little control over corporate actions and the handling of personal data by online services.

We define "privacy cynicism" as ***an attitude of uncertainty, powerlessness and mistrust towards the handling of personal data by online services, rendering privacy protection behavior subjectively futile***. An attitude of privacy cynicism can be understood as a cognitive coping mechanism in the context of the "privacy paradox" because it allows fearful, low-skilled users to take advantage of the desired online services without cognitive dissonance since privacy protection behavior can be rationalized as useless or ineffective. Given this definition, we would expect privacy cynicism attitudes to be negatively related to Internet literacy, privacy protection skills and self-efficacy (cf., Milne, Labreque, & Cromer, 2009; Park, 2013), as high-skilled users should feel less powerless vis-à-vis service providers. Just as the trust concept has been differentiated into trusting dispositions and trusting beliefs (McKnight et al., 2002), it could be argued that privacy cynicism combines elements of both a trait and state, as individuals may be more or less cynical by nature, but may also develop varying levels of cynicism over time due to specific perceptions and experiences. These relationships and differentiations go beyond the scope of this initial analysis, though. In the following pages, we proceeded to empirically explore the phenomenon of privacy cynicism to substantiate the concept. In the conclusion, we will then propose a nomological network of the concept.

Methods

In late 2014, we conducted focus groups and online discussion groups with a wide range of Internet users, discussing Internet use and online participation in Germany. 96 users participated in the focus groups which took place in September 2014. Twelve focus groups were carried out, with eight participants per group. The aim of this study was to discuss and explore German Internet users' Internet use and online participation. Six focus groups took place in Berlin and six in Frankfurt. Each focus group was composed of a different age and social profile. The groups were recruited based on a representative typology of German Internet users that differentiates seven distinct user types or Internet milieus (DIVSI, 2012). This milieu categorization goes back to the "Sinus-Milieus®", which were developed in the 1980ies by the German market and social science research company Sinus. Subsequently, the Sinus-Milieus® were applied in many contexts and for various questions, mainly in the German-speaking world [Gröger, Schmid and Bruckner (2011) offer a summary in English, and Otte (2004) evaluates the typology in German].

Two of the seven types can be categorized as digital outsiders: elderly people who hardly use the Internet and are cautious and inexperienced in using Internet applications. These types were analyzed with one focus group each. The remaining five types are characterized by more open attitudes towards the Internet. They can be categorized as either digital natives or digital immigrants (Prensky, 2001) and were analyzed with two focus groups each. Appendix A gives an overview of the seven milieus and Figure A1 shows a graphical depiction (in German). The focus groups were moderated by two experienced employees of a cooperating German social research institute. Four additional members of the research team observed the conversations but did not actively intervene during the discussions.

For the online discussion groups, an additional 18 individuals were recruited to participate based on the same sampling scheme to compensate for the higher drop-out rate of online groups. Thereby, 38 representatives each of the digital natives, immigrants, and outsiders initially participated in the online discussion groups, which ran over the course of ten days in the beginning of October 2014. We used a dedicated qualitative research platform (Kernwert, http://www.kernwert.com/) for the online discussion groups and two members of the research team moderated the online discussion groups after a detailed training session by the platform provider. Each day, participants carried out a small task, such as describing their daily Internet use or discussing a negative (*I do not participate online because I'm afraid of losing control over my personal data*) and a positive statement (*I participate online because I can learn something and useful and because I can help others*) with the other participants in the online discussion groups. A detailed description of the focus groups and online discussion groups as well as the results of the overall projects is available in Hoffmann, Lutz, & Poëll (2015). In total, 18 participants did not finish all tasks so that eventually, the data of 96 active members of the online discussion groups were considered for analysis.

The focus groups were recorded on video and audio and transcribed. Three members of the research team, all experienced communication science researchers, each scanned all focus group transcripts and online discussion group log files independently for statements referring to online privacy. We relied on the focus group guideline as the main structuring element (Appendix C), inspired by current focus group studies (e.g., Hargittai, Neuman, & Curry, 2012). The identified statements were initially categorized as referring to privacy attitudes or behavior. In a second step, statements were selected and coded if they were found to refer to aspects of cynicism as identified in the literature review described above. The resultant subset was discussed by the research team, which agreed upon a division or merging of categories where necessary. The resultant four categories are discussed below, substantiated by illustrative quotes. The original quotes were in German and translated to English for this article (original German wording in Appendix A).

Results

During the focus group discussions of online privacy, Internet use and online participation, we identified four recurring themes that all indicate elements of privacy cynicism corresponding with elements of cynicism identified in the literature: uncertainty and insecurity, loss of control/powerlessness, mistrust, and resignation.

A number of comments refer to ***insecurity and uncertainty*** when it comes to Internet use and online privacy, across all milieus considered: *"I think, as soon as you do anything online, you will leave traces of data, and people who want to find out about you will do so – even if I didn't want to publish that information. So it's really no use being afraid of sharing data."* (Q1) Many participants reported a lack of understanding, particularly those less skilled and experienced. In these instances, users feel helpless when faced with little understood sinister forces threatening online privacy: *„People like us who use Facebook and shop online etc. have already divulged so much information, so any hacker could do you harm. So, I don't really care what I post online, I am just one among many and the risk is unavoidable. Although I would prefer not to be part of the Internet, but that's simply not possible nowadays".* (Q2) This lends support to the notion that user skills and self-efficacy may be negatively related to privacy cynicism.

Powerlessness or loss of control is another important recurring theme. Faced with overwhelming forces – or corporations/services – shaping the Internet, many users feel they can't really affect the use and spread of personal data: *„A couple of days later I read in the media that PayPal had been hacked or something. I was left with the feeling 'you better should have left that be'. By now, so many of my data are buzzing around online, I really can't reverse that. In my opinion, nobody who uses eBay, Amazon or a service like that has any control."* (Q3) Again, this element of cynicism is closely related to a lack of efficacy: *„I always hesitated to participate online and share data. But even if you try to avoid that, for example by using nicknames, you still can be tracked, your connection from which you connect to the Internet, how long you visit which pages etc. You reveal data that you really don't want to share. In the end, you can't really influence that if you're not an expert."* (Q4)

Interestingly, among more savvy Internet users, we found indications that literacy may not necessarily be negatively related to cynicism. Higher levels of risk awareness may lead some skilled users to more readily resort to resignation: *„I think control, for a regular citizen, is hypocrisy, just so we can feel better. Just among the people I know, because I work on PCs, I have access to so much personal data. People tell me how important it is to have security software and all that so their data are secure. But then they share their passwords, credit card details and anything I want. I you are inexperienced, you can live in the illusion that your data are secure. If you are experienced, you know that it's simply too much effort to encode everything."* (Q5)

Many participants described feelings of ***mistrust*** towards those agents shaping the online environment, including large online service providers: *"Who seriously believes you have control over your data online? Every movement, every click is recorded by someone, analyzed. All data are used to make money in some way or another, to gain power, to instill fear or control."* (Q6) Again, users speculate about selfish and sinister motives of these agents – an attitude prevalent among both high- and low-skilled participants. Past negative experience appears to increase the salience of this cynicism-element: *„It's an illusion to think you can protect yourself. You received junk mail even before the Internet existed, although you never shared you address. Everybody who has a Facebook account, online banking or eBay has lost his or her data to those data collectors."* (Q7) While mistrust towards service providers is a common occurrence, many users also voice skepticism regarding the motives of other users:

„Common users like us who do online shopping, plan vacations, book flights, do online banking, social networks, e-mails, VoIP etc. have left such a large virtual data footprint and revealed so many data that shrewd users or those who want to use your data can access it without problem." (Q8)

Finally, mistrust towards online services, insecurity and a feeling of powerlessness come together in an attitude of ***resignation***. A number of participants flat-out state that privacy protection is futile, which in turn to leads to more open, possibly even careless self-disclosure practices: *„I'm quite careless with my data. It's illogical to think that you can somehow obfuscate your digital footprint given the number of activities we do online. You would have to become some kind of dropout living in the mountains."* (Q11) Some feel that there is no viable alternative to using the Internet and large online services, and that these services cannot be controlled and personal data cannot effectively be protected: *„You can't really get along without the Internet, it takes ever more space in your daily live, respectively: you are pulled into it. As a customer in a shop that only offers certain products online or as customer of a bank that pushes you towards an online account. You cannot prevent it."* (Q9)

Thereby, cynical users justify to themselves the fact that they do not even seriously attempt to protect their privacy online, illustrating the role of cynicism as a coping mechanism: *„By now, I really don't think much about it anymore. Sure, you have to be careful. At the same time, you don't have any control over your data. Even if you unsubscribe a service, your data are still out there."* (Q10)

Discussion

Our analysis aims to enrich the current debate on privacy by introducing the concept of privacy cynicism, which we believe could be particularly useful to understand the re-definition of privacy boundaries taking place in the last years, mostly as a response to several scandals involving companies, governments and private user data. While the exposure of institutional programs of data espionage such as PRISM attracted significant media attention and public debate, the online behavior of citizens seems largely unaffected. One possible explanation could be that the shock and outrage of citizens might have blended into a state of resignation, as being online could inevitably be associated with privacy threats.

We have described this attitude as privacy cynicism, defined it based on a literature review and empirically substantiated the concept based on the outcomes of several focus groups. Both high and low-skilled Internet users participating in the focus groups highlighted a mixture of mistrust and feelings of privacy vulnerability as well as powerlessness related to the experience of being online. The concept as developed in this analysis is inspired by the proposition that privacy cynicism might contribute to an explanation of the observed disparities between many users' privacy attitudes and behavior (Acquisti, 2004, Tufekci, 2008). Since digital devices, various online services and usage contexts make the control of privacy settings increasingly complicated, users may be lead to believe any protection effort to be substantially useless.

We describe privacy cynicism as a coping mechanism to an objective situation of risk, where scandals have undermined the trust users invested in service providers and institutions at large (Lutz & Strathoff, 2013). Privacy cynicism allows users to take advantage of online services without trusting their providers and while aware of privacy threats by forming the conviction that effective privacy protection is out of their hand. By ascribing responsibility for foreseeable damage to unavoidable and overwhelming external forces, users avoid cognitive dissonance while engaging in seemingly paradoxical behavior. We propose that privacy cynicism could be particularly critical if combined with low Internet skills and self-efficacy: cynicism might facilitate risky behavior, as opportunities to develop skills or employ protection mechanisms are increasingly forgone. In the long run, cynicism could contribute to another skills divide, where those who are poor in skills only get poorer.

This research represents a first attempt at the conceptualization of privacy cynicism and is hence to be treated essentially as the start of a conversation on a new concept. Future studies will have to further explore the nomological network of the concept (see Figure 1). Given our description above, we propose that privacy cynicism moderates (i.e., weakens) the effect of privacy concerns on protection behavior. In turn, this may facilitate more open and comprehensive online self-disclosure (Metzger, 2004; Kane, Alavi, Labianca, & Borgatti, 2014). Given that the concept of privacy cynicism as developed in this paper focuses on institutional privacy threats, it would be worthwhile to explore its salience and effects in different use contexts, for example by

comparing services such as e-commerce, online search, SNS etc. In the SNS context, in particular, taking privacy cynicism into consideration could offer interesting insights into the type and amount of self-disclosure users decide to engage in given various levels of cynicism (Dienlin & Metzger, 2016).

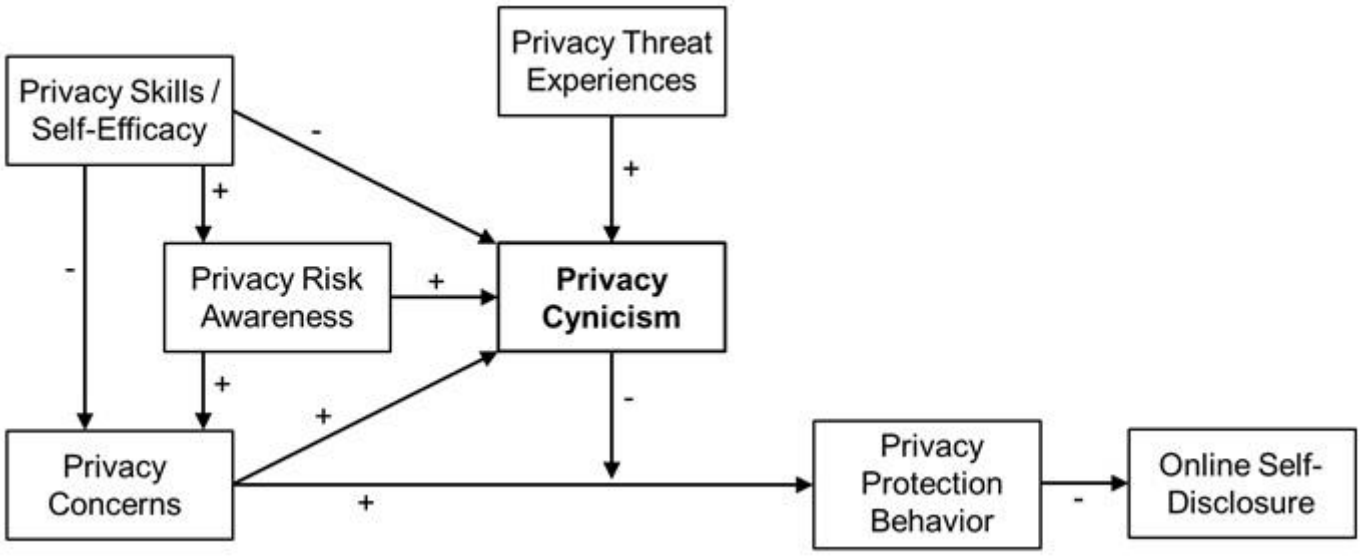

Figure 1. Nomological network of privacy cynicism.

Future research should also examine the relationship between privacy skills or self-efficacy and cynicism. We propose that privacy self-efficacy might render privacy threats more manageable (Park, 2013), thereby reducing privacy concerns and the need for cynicism (Dinev & Hart, 2005). At the same time, high-skilled users may be more aware of privacy threats (Smith, Dinev & Xu, 2011), which may increase both privacy concerns and the propensity to resort to privacy cynicism. Our focus group data provided evidence of both effects. Taking user efficacy, trust, and cynicism into account may allow for a more comprehensive analysis of the purported "privacy paradox".

While privacy cynicism does have trait-like qualities, negative privacy experiences might aggravate it. Since the privacy cynicism concept emerged, at least in part, as a consequence of scandals of surveillance and data leaks, future studies could approach the matter longitudinally, allowing for a deeper analysis of the evolution of individual perceptions and public discourses on privacy risks, behavior and cynicism. Psychological studies may delve deeper into personal antecedents of cynicism, such as socio-economic variables or personality traits. We describe privacy cynicism as a coping mechanism when faced with privacy threats, yet a range of alternative mechanism may be chose depending on user traits or attitudes (e.g., avoidance or anger).

The concept of privacy cynicism offers interesting implications, both in terms of practice and policy. We would expect dominant service providers with large market shares to engender more privacy cynicism. Moreover, provider reputation should affect privacy cynicisms, as providers with questionable reputations attracting critical public scrutiny but still commanding dominant market shares should increase users' feeling both of mistrust and powerlessness. Large providers, therefore, should be aware that a large user base may not signify user trust or sympathy. As privacy cynicism is a new concept, little is known about the sustainability of business models heavily reliant on user cynicism.

We also believe that institutions and governments should pay attention to privacy cynicism, as individuals who are cynical about their online privacy might not limit their lack of trust to Internet service providers, especially if they feel unprotected or ignored. Cynical attitudes may therefore spread to other domains, such as media or politics. Furthermore, the collective economic and social benefits of digital media may be compromised if ever more extensive use comes at the cost of ever higher levels of user cynicism.

As an initial conceptual analysis of privacy cynicism, this study is associated with a number of limitations that invite further research: the results of the focus groups primarily serve to explore and characterize the concept, rather than delve into causal relationship. Quantitative analyses would lend themselves to explorations of the relationships outlined above. As privacy is a concept strongly influenced by culture, we also expect future research to operate cross-culturally. Finally, we believe that privacy cynicism is not only an aspect worthy of investigation as an element affecting online experiences, but an interesting lens through which to interpret the seemingly paradoxical deviation of privacy protection behavior from privacy concerns. Taking privacy cynicism into consideration could provide a psychological understanding that is not based on a disparity between attitudes and behavior, but rather on an adaptation of attitudes to perceived circumstances allowing for an avoidance of cognitive dissonance. We hope to soon extend our research on privacy cynicism, and invite fellow privacy researchers to take the concept into consideration.

References

Acquisti, A. (2004). Privacy in electronic commerce and the economics of immediate gratification. In *Proceedings of the 5th ACM Electronic Commerce Conference* (pp. 21-29). New York, NY: ACM. http://dx.doi.org/10.1145/988772.988777

Ajzen, I. (1991). The theory of planned behavior. *Organizational Behavior and Human Decision Processes, 50*, 179–211. http://dx.doi.org/10.1016/0749-5978(91)90020-T

Almada, S. J., Zonderman, A. B., Shekelle, R. B., Dyer, A. R., Daviglus, M. L., Costa, P. T., & Stamler, J. (1991). Neuroticism and cynicism and risk of death in middle-aged men: The Western Electric Study. *Psychosomatic Medicine, 53*, 165-175.

Andersson, L. M. (1996). Employee cynicism: An examination using a contract violation framework. *Human Relations, 49*, 1395-1418. http://dx.doi.org/10.1177/001872679604901102

Barnes, S. B. (2006). A privacy paradox: Social networking in the United States. *First Monday, 11*(9). http://dx.doi.org/10.5210/fm.v11i9.1394

Bartsch, M., & Dienlin, T. (2016). Control your Facebook: An analysis of online privacy literacy. *Computers in Human Behavior, 56*, 147-154. http://dx.doi.org/10.1016/j.chb.2015.11.022

Bhattacherjee, A. (2002). Individual trust in online firms: Scale development and initial test. *Journal of Management Information Systems, 19*, 211-241. http://dx.doi.org/10.1080/07421222.2002.11045715

boyd, d., & Hargittai, E. (2010). Facebook privacy settings: Who cares? *First Monday, 15*(8). http://dx.doi.org/10.5210/fm.v15i8.3086

Cappella, J. N., & Jamieson, K. H. (1996). News frames, political cynicism, and media cynicism. *Annals of the American Academy of Political and Social Sciences, 546*, 71-84. http://dx.doi.org/10.1177/0002716296546001007

Dean, J. W., Brandes, P., & Dharwadkar, R. (1998). Organizational cynicism. *The Academy of Management Review, 23*, 341-352. http://dx.doi.org/10.2307/259378

Dienlin, T., & Metzger, M. J. (2016). An extended privacy calculus model for SNSs: Analyzing self-disclosure and self-withdrawal in a representative U.S. sample, *Journal of Computer-Mediated Communication*. Advance online publication. http://dx.doi.org/10.1111/jcc4.12163

Dienlin, T., & Trepte, S. (2015). Is the privacy paradox a relic of the past? An in-depth analysis of privacy attitudes and privacy behaviors. *European Journal of Social Psychology, 45*, 285-297. http://dx.doi.org/10.1002/ejsp.2049

Dinev, T., & Hart, P. (2005). Internet privacy concerns and social awareness as determinants of intention to transact. *International Journal of Electronic Commerce, 10*(2), 7-29. http://dx.doi.org/10.2753/jec1086-4415100201

Dinev, T., & Hart, P. (2006). An extended privacy calculus model for e-commerce transactions. *Information Systems Research, 17*(1), 61–80. http://dx.doi.org/10.1287/isre.1060.0080

DIVSI (2012). *Milieu-Studie zu Vertrauen und Sicherheit im Internet* [Milieu study about trust and security on the Internet]. Retrieved from https://www.divsi.de/sites/default/files/presse/docs/DIVSI-Milieu-Studie_Gesamtfassung.pdf

DIVSI (2013). *Milieu-Studie zu Vertrauen und Sicherheit im Internet – Aktualisierung 2013* [Milieu study about trust and security on the Internet – Update]. Retrieved from https://www.divsi.de/wp-content/uploads/2013/12/DIVSI_Milieu-Studie_Aktualisierung_2013.pdf

Festinger, L. (1957). *A theory of cognitive dissonance*. Palo Alto, CA: Stanford University Press.

Gröger, M., Schmid, V., & Bruckner, T. (2011). Lifestyles and their impact on energy-related investment decisions. *Low Carbon Economy, 2*(2), 107-114. http://dx.doi.org/10.4236/lce.2011.22014

Hargittai, E., & Litt, E. (2013). New strategies for employment? Internet skills and online privacy practices during people's job search. *IEEE Security & Privacy, 3*, 38-45. http://dx.doi.org/10.1109/msp.2013.64

Hargittai, E., Neuman, R. W., & Curry, O. (2012). Taming the information tide: Perceptions of information overload in the American home. *The Information Society, 28*, 161-173. http://dx.doi.org/10.1080/01972243.2012.669450

Hoffman, D. L., Novak, T. P., & Peralta, M. (1999). Building consumer trust online. *Communications of the ACM, 42*(4), 80-85. http://dx.doi.org/10.1145/299157.299175

Hoffmann, C. P., Lutz, C., & Poëll, R. (2015). *DIVSI-Studie: Beteiligung im Internet: Wer beteiligt sich wie?* [DIVSI study: Participation on the Internet. Who participates how?]. Retrieved from https://www.divsi.de/wp-content/uploads/2015/07/DIVSI-Studie-Beteiligung-im-Internet-Wer-beteiligt-sich-wie_web.pdf

Hoofnagle, C. J., King, J., Li, S., & Turow, J. (2010, April). How different are young adults from older adults when it comes to information privacy attitudes and policies? *SSRN*. http://dx.doi.org/10.2139/ssrn.1589864

Hurwitz, J. B. (2013). User choice, privacy sensitivity, and acceptance of personal information collection. In *European data protection: Coming of age* (pp. 295-312). Springer Netherlands. http://dx.doi.org/10.1007/978-94-007-5170-5_13

Jarvenpaa, S. L., Tractinsky, N., & Vitale, M. (2000) Consumer trust in an Internet store. *Information Technology and Management, 1*(1-2), 45-71. http://dx.doi.org/10.1023/a:1019104520776

Kane, G. C., Alavi, M., Labianca, G., & Borgatti, S. P. (2014). What's different about social media networks? a framework and research agenda. *MIS Quarterly, 38*, 274-304.

Kanter, D. L., & Mirvis, P. H. (1989). *The cynical Americans: Living and working in an age of discontent and disillusion*. Jossey-Bass.

Klara, R. (2016, January 21). How big a problem is it for Google and Facebook that consumers don't trust them? 2 Web brands rank surprisingly low in relevance survey. *AdWeek*. Retrieved from http://www.adweek.com/news/advertising-branding/how-big-problem-it-google-and-facebook-consumers-don-t-trust-them-169108

Kokolakis, S. (2017). Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. *Computers & Security, 64*, 122-134. http://dx.doi.org/10.1016/0047-2352(87)90075-4

Krasnova, H., Spiekermann, S., Koroleva1, K., & Hildebrand, T. (2010). Online social networks: why we disclose. *Journal of Information Technology, 25*, 109–125. http://dx.doi.org/10.1057/jit.2010.6

Krasnova, H., Veltri, N. F., & Günther, O. (2012). Die Rolle der Kultur in der Selbstoffenbarung und Privatsphäre in sozialen Onlinenetzwerken [The role of culture in self-disclosure and privacy on social network sites]. *WIRTSCHAFTSINFORMATIK, 54*(3), 123-133. http://dx.doi.org/10.1007/s11576-012-0323-5

Langworthy, R. H. (1987). Police cynicism: What we know from the Niederhoffer scale. *Journal of Criminal Justice, 15*(1), 17-35. http://dx.doi.org/10.1016/0047-2352(87)90075-4

Lanier, C. D., & Saini, A. (2008). Understanding consumer privacy: A review and future directions. *Academy of Marketing Science Review, 12*(2), 1–45.

Lee, H., Park, H., & Kim, J. (2013). 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, 71*, 826-877. http://dx.doi.org/10.1016/j.ijhcs.2013.01.005

Lutz, C., & Strathoff, P. (2013). Privacy concerns and online behavior – Not so paradoxical after all? Viewing the privacy paradox through different theoretical lenses. In S. Brändli, R. Schister, & A. Tamo (Eds.), *Multinationale Unternehmen und Institutionen im Wandel – Herausforderungen für Wirtschaft, Recht und Gesellschaft* [Changing multi-national companies and institutions – Challenges for economy, law, and society] (pp. 81-99). Bern: Stämpfli. Retrieved from https://papers.ssrn.com/sol3/Papers.cfm?abstract_id=2425132

McKnight, D. H., Choudhury, V., & Kacmar, C. (2002). Developing and validating trust measures for e-commerce: An integrative typology. *Information Systems Research, 13*, 334-359. http://dx.doi.org/10.1287/isre.13.3.334.81

Metzger, M. J. (2004). Privacy, trust, and disclosure: Exploring barriers to electronic commerce. *Journal of Computer-Mediated Communication, 9*(4). http://dx.doi.org/10.1111/j.1083-6101.2004.tb00292.x

Mills, C. M., & Keil, F. C. (2005). The development of cynicism. *Psychological Science, 16*, 385-390. http://dx.doi.org/10.1111/j.0956-7976.2005.01545.x

Milne, G. R., Labreque, L. I., & Cromer, C. (2009). Toward an understanding of the online consumer's risky behavior and protection practices. *The Journal of Consumer Affairs, 43*, 449-473. http://dx.doi.org/10.1111/j.1745-6606.2009.01148.x

Otte, G. (2004). *Sozialstrukturanalysen mit Lebensstilen – Eine Studie zur theoretischen und methodischen Neuorientierung der Lebensstilforschung* [Social structure analysis with lifestyles – A study for the theoretical and methodical re-orientation of lifestyle research]. Wiesbaden: VS Verlag für Sozialwissenschaften. http://dx.doi.org/10.1007/s11577-005-0157-x

Park, Y. J. (2013). Digital literacy and privacy behavior online. *Communication Research, 40*, 215-236. http://dx.doi.org/10.1177/0093650211418338

PEW Research (2014): *Public perceptions of privacy and security in the post-Snowden era*. Retrieved from http://www.pewinternet.org/files/2014/11/PI_Public PerceptionsofPrivacy_111214 .pdf

Prensky, M. (2001). Digital natives, digital immigrants part 1. *On the horizon, 9*(5), 1-6. http://dx.doi.org/10.1108/10748120110424816

Raynes-Goldie, K. (2010). Aliases, creeping, and wall clearning: Understanding privacy in the age of Facebook. *First Monday, 15*(1). http://dx.doi.org/10.5210/fm.v15i1.2775

Regoli, R. (1976). An empirical assessment of Niederhoffer's police cynicism scale. *Journal of Criminal Justice, 4*, 231-241. http://dx.doi.org/10.1016/0047-2352(76)90005-2

Rousseau, D. M., Sitkin, S. B., Burt, R. S., & Camerer, C. (1998). Not so different after all: A cross-discipline view of trust. *Academy of Management Review, 23*, 393-404. http://dx.doi.org/10.5465/amr.1998.926617

Salanova, M., Llorens, S., Garcia-Renedo, M., Burriel, R., & Bresc, E. (2005). Toward a four-dimensional model of burnout: A multigroup factor-analytical study including depersonalization and cynicism. *Educational and Psychological Measurement, 65*, 901-913. http://dx.doi.org/10.1177/0013164405275662

Smith, H. J., Dinev, T., & Xu, H. (2011). Information privacy research: An interdisciplinary review. *MIS Quarterly, 35*, 989-1016.

Smith, T. W., & Pope, M. K. (1990). Cynical hostility as a health risk: Current status and future directions. *Journal of Social Behavior and Personality, 22*, 525-548.

Trepte, S., Teutsch, D., Masur, P. K., Eicher, C., Fischer, M., Hennhöfer, A., & Lind, F. (2015). Do people know about privacy and data protection strategies? Towards the "Online Privacy Literacy Scale"(OPLIS). In S. Gutwirth, R. Leenes, & P. de Hert (Eds.), *Reforming European data protection law* (pp. 333-365). Dordrecht: Springer Netherlands.

Tufekci, Z. (2008). Grooming, gossip, Facebook and MySpace: What can we learn about these sites from those who won't assimilate? *Information, Communication & Society, 11*, 544–564. http://dx.doi.org/10.1080/13691180801999050

Turner, J. H., & Valentine, S. R. (2001). Cynicism as a fundamental dimension of moral decision-making: A scale development. *Journal of Business Ethics, 34*, 123-136. http://dx.doi.org/10.1023/a:1012268705059

Valentino, N. A., Beckmann, M. N., & Buhr, T. A. (2001). A spiral of cynicism for some: The contingent effects of campaign news frames on participation and confidence in government. *Political Communication, 18*, 347-367. http://dx.doi.org/10.1080/10584600152647083

Young, A., & Quan-Haase, A. (2013). Privacy protection strategies on Facebook: The Internet privacy paradox revisited. *Information, Communication & Society, 16*, 479–500. http://dx.doi.org/10.1080/1369118x.2013.777757

Appendices

Appendix A: German Original Version of Quotes

Q1: *Ich denke, dass, sobald man irgendwie irgendwas im Internet macht, seine spuren hinterlassen hat, und derjenige, der etwas über mich rausfinden will, es auch ohne von mir eigens angegebenen Daten tun kann. Daher habe ich keine Angst irgendwelche Daten (ausgenommen von Kontonummer) preis zu geben.*

Q2: *Wir die Facebook nutzen und Onlineeinkäufe etc. erledigen haben schon so viel von sich preis gegeben dass ein Hacker genug Daten hat, um dich fertig machen zu können. Es ist mir also eher egal, was ich im Internet poste, da ich nur einer von vielen bin und dieses Risiko eben eingehe. Allerdings wäre ich am liebsten komplett aus dem Internet entkuppelt, aber dies ist ja nicht mehr so einfach heutzutage.*

Q3: *Einige Tage später gab es Medienmitteilungen, dass PayPal von Hackern auch "geknackt" worden war. Nun blieb bei mir das Gefühl: "Hättest du das doch besser gelassen". Nun jedoch schwirren schon so viele Daten von mir im Internet herum, dass ich dies nicht mehr rückgängig machen kann. Meiner Meinung nach hat niemand, der im Internet eBay, Amazon etc. oder Versandhäuser benutzt, irgendeine Kontrolle.*

Q4: *Bisher war ich immer zögerlich, mich am Internet zu beteiligen und bewusst Daten weiterzugeben. Aber auch wenn man versucht, das zu vermeiden und z.B. Nicknames benutzt, kann ja verfolgt werden, von welchem Anschluss aus man*

ins Internet geht, wie lange man auf welchen Seiten ist usw. Dadurch gibt man Daten preis, die man eigentlich gar nicht weitergeben wollte. Letztlich kann man das kaum beeinflussen, jedenfalls dann nicht, wenn man, wie ich, computertechnisch weitgehend Laie ist.

Q5: *Ist Kontrolle nicht für den Normalbürger was Geheucheltes, damit er sich besser fühlt? Ich habe alleine in meinem Umfeld zu so vielen Privaten Daten Zugriff, nur dadurch, dass ich PCs von anderen mal überarbeitet habe. Die Leute erzählen mir immer wie wichtig es ist, Virenscanner und dies und jenes drauf zu machen, damit niemand an ihre Daten kommt. Dann im nächsten Moment geben sie mir Passwörter, Kreditkarten und alles was ich will. Wenn die Leute sich nicht auskennen, dann leben sie nur in einem Glauben, dass ihre Daten sicher sind. Wenn die Leute sich auskennen, merkt man, es ist einfach zu viel Arbeit, alles zu verschlüsseln.*

Q6: *…Wer glaubt denn noch wirklich, dass er die Kontrolle über seine Daten im Internet/Leben hat!? Jede Bewegung / jeder Klick im Internet/Leben wird von irgendjemand irgendwo festgehalten, analysiert, in Statistiken ausgewertet! Diese Daten dienen entweder im nahen oder weiterem Sinne: das Geld zu mehren; Macht zu erlangen; Ängste zu verbreiten und zu kontrollieren!*

Q7: *Das ist doch ne totale Illusion, dass man sich so davor schützen kann! Man hat auch vor dem Internet schon Werbung per Post bekommen, obwohl man denen nie seine Adresse gegeben hat. Jeder, der einen Facebookaccount hat oder Onlinebanking oder eBay macht, hat seine Daten schon an die Datenkrake verloren…*

Q8: *Ich bin der Meinung, dass wir selbst als Otto Normalverbraucher im Internet durch Online-Shopping, Urlaubsbuchungen, Flugbuchungen, Onlinebanking, Soziale-Netzwerke, Emails, Voip, usw. längst einen so gro_en virtuellen Fu_abdruck hinterlassen und soviele Daten von uns preis geben, dass geübte Hacker oder Personen, die diese Daten wirklich interessieren, ohne grö_ere Probleme darauf Zugriff haben.*

Q9: *Ich bin der Meinung, dass man ohne Internet nicht mehr auskommt und es immer mehr in unseren Alltag tritt bzw. wir dort immer mehr hingezogen werden. Sei es als Kunden eines Store, der bestimmte Angebote nur noch online bietet oder als Kunde einer Bank, die Ihren Kunden mit Online-Konto bestimmte Vorteile bietet. Wir können es nicht verhindern.*

Q10: *Also, ich mache mir mittlerweile nicht so viele Gedanken darüber. Eins ist jedoch klar, man muss schon vorsichtig sein. Es ist aber auch klar, dass man leider keine Kontrolle über die persönlichen Daten hat, denn auch wenn man sich irgendwo ganz abmeldet, bleiben die Daten gespeichert.*

Q11: *Ich bin sehr locker im Umgang mit Daten. Es ist doch unlogisch zu denken, man könne seinen digitalen Fu_abdruck irgendwie verwischen, bei der Anzahl an Aktivitäten bzw. Beteiligung im Internet. Da muss man wohl als Aussteiger auf einer Alm leben ;)*

Appendix B: Description of the Internet Milieus

The Internet milieus were first established in a large-scale German-wide study on Internet use in Germany (DIVSI, 2012) and subsequently reaffirmed in a follow-up survey one year later (DIVSI, 2013). The focus group participants in this article were recruited along the Internet milieus by the cooperating market and social science research institute. The Internet milieus are largely in line with the older concept of Sinus-Milieus®, developed in the 1980ies (Otte, 2004; Gröger et al., 2011). The Internet milieu typology was originally developed in two steps: with 60 qualitative interviews in a first step and a large face-to-face (computer-assisted) survey with 2047 respondents in a second step. The survey was representative of the German population aged 14 and older. The Internet milieus were constructed with a cluster analysis from the quantitative data, based on three main factors: Sinus-Milieu® membership, Internet use, and data protection/privacy attitudes. For more information on the methodological construction of the original typology see DIVSI (2012, pp. 19-34).

Digital natives.

Immersed natives / Digital Souveräne (16 percent of Internet users in Germany):

- Age: below 40 (youngest milieu of all)
- Education: highest level of education of all groups
- Income: high level of income
- Occupation: often in media and creative industries, often self-employed
- Elevated postmodern milieu, pronounced performance ethos and elite consciousness
- High technology enthusiasm, high Internet use intensity, broad spectrum of online activities, high level of computer and Internet skills

Selective natives / Effizienzorientierte Performer (16 percent of Internet users in Germany):

- Age: below 50 (On average: 40 years old)
- Education: high level of education
- Income: highest level of income of all groups
- Occupation: many self-employed, large part of medium/skilled employed and upper public administration professionals
- Performance-oriented milieu, success-driven, optimistic performance stance and life stance, let's do it approach, self-confidence as modern top performers
- High technology enthusiasm, high Internet use intensity, broad spectrum of online activities, high level of computer and Internet skills

Entertainment-oriented natives / Unbekümmerte Hedonisten (12 percent of Internet users in Germany):

- Age: younger and middle-aged group (On average: 42 years old)
- Education: predominantly low level of education
- Income: intermediate level of income
- Education: less skilled to medium-skilled service employees, workers and crafts(wo)men
- Hedonistic milieu, orientation towards enjoyment, experience and excitement, underdog mentality
- Quite high technology enthusiasm, high Internet use intensity, rather broad spectrum of online activities, average/intermediate level of computer and Internet skills

Digital immigrants.

Detached immigrants / Verantwortungsbedachte Etablierte (10 percent of Internet users in Germany):

- Age: broad age spectrum, centering on 30 to 50 years old
- Education: high level of education
- Income: intermediate to high level of income
- Occupation: mostly high-level service employed and upper public administration
- Conservative and established milieu, liberal intellectual attitudes, elite consciousness, optimistic performance stance and life stance
- Intermediate technology enthusiasm, rather high Internet use intensity, rather broad spectrum of uses, rather high level of computer and Internet skills

Skeptical immigrants / Postmaterielle Skeptiker (9 percent of Internet users in Germany):

- Age: very broad spectrum from 20 to 60 (On average: 45 years old)
- Education: primarily low level of education
- Income: intermediate level of income
- Occupation: qualified employees, workers and skilled workers, self-employed
- Social-ecological milieu, ecologically ambitious middle of society, sustainable lifestyle, high willingness to refrain from luxury

- Low technology enthusiasm, rather high Internet use intensity, rather broad spectrum of online activities, rather high level of computer and Internet skills

Digital outsiders.

Law-and-order outsiders / Ordnungsfordernde Internetlaien (10 percent of Internet users in Germany):

- Age: predominantly between 40 and 70 (On average: 51 years old)
- Education: lower to intermediate level of education
- Income: low to intermediate level of income
- Occupation: predominantly part-time employed, housewifes/homemakers, retirees, unemployed, and low/intermediate skilled employees and workers
- Conservative-established milieu, civic middle class, harmony orientation, preference for safety and protection
- Low technology enthusiasm, intermediate Internet use intensity, intermediate spectrum of online activities, low level of computer and Internet skills

Internet-distanced outsiders / Internetferne Verunsicherte (27 percent of Internet users in Germany):

- Age: highest age of all groups (On average: 62 years old)
- Education: low level of education
- Income: low level of income
- Occupation: high proportion of retirees, basic professions, workers and skilled workers
- Traditional and precarious milieu, need for straightforwardness, clarity and security, resignation and pessimism towards the future
- Low technology enthusiasm, low Internet use intensity, small spectrum of online activities, low level of computer and Internet skills

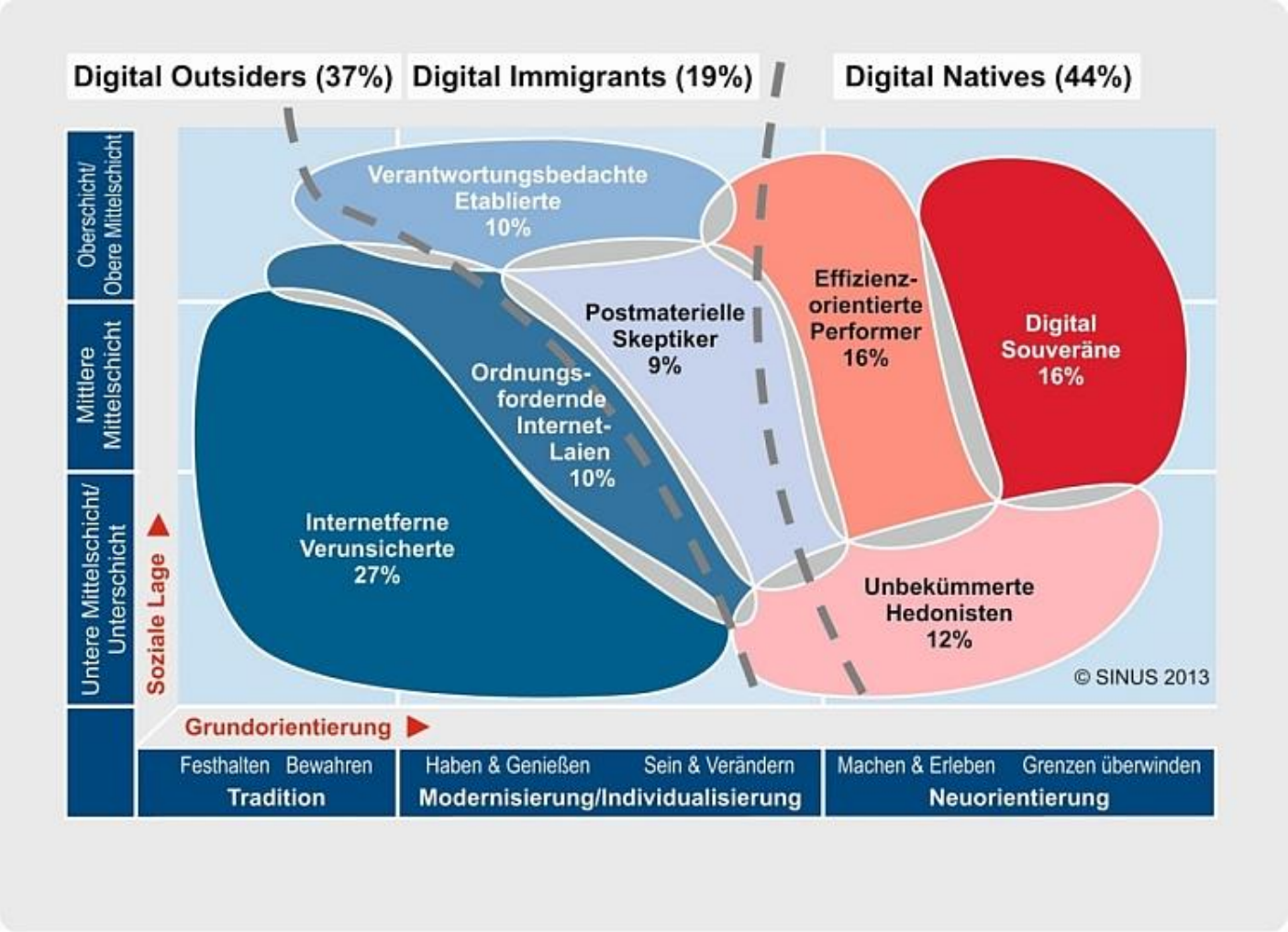

Figure A1. Overview of the seven Internet Milieus (DIVSI, 2013). The vertical axis describes individuals' SES, ranging from working class to middle class, to upper class. The horizontal axis describes attitudes and orientations, ranging from traditional and conserving on the left, to modernization/individualization in the middle, to re-orientation and realignment on the right.

Appendix C: Focus Group Guideline

This is a summarized version of the guideline. A more detailed version is available upon request.

Introduction: General attitude towards the Internet.

- What does the Internet mean to you?
- What are the major advantages and disadvantages of the Internet?

Internet use.

- Since when do you use the Internet?
- How often do you use the Internet?
- How much time per day do you spend using the Internet?
- Which devices do you use to access the Internet?
- What do you do when you are online? Which platforms do you use?
- For which purposes do you use the Internet? (Also: Do you sometimes go
- online without a concrete purpose in mind?)
- Do you find using the Internet easy? Where are your limits?

- How do people in your social environment use the Internet?
- Do you have friends who use the Internet very actively? How does that show?
- *→Collection on Flipchart: forms of Internet use and activities*

Social Internet use/Self-Disclosure.

- How important is the exchange with others for your Internet use?
- Are you active in online communities? (If not: why not?)
- How often do you post texts, videos and photos online? What kind of texts, videos and photos?
- Who do you post texts, videos and photos to (which audience)?
- Do you know the people you communicate with online (from the offline world)?
- Are there things you only do on the Internet, and nowhere else?
- What things would you not do on the Internet? / Are there things you would only do offline?
- *→Collection on Flipchart: social forms and activities of Internet use*

Online participation.

- What does „participation", in general, mean to you?
- What does online participation mean to you?

Assocation spaces / Semantic fields of online participation

Areas/Domains of online participation.

- *→Carefully support the areas emerging from the addition to be able to assess not mentioned but existing aspects (education, business, sports, cultural participation…)*
- Which other areas/domains/fields of participation can you think of?
- Where do you participate online?
- Who is the public/recipient of your online participation activities?
- Where are your friends and colleagues participating?
- *→Sorting forms of participation on a continuum according to the depth/quality of participation*
- Which are the most important areas of participation on the Internet? (ca. 3)

Chances and risks of online participation.

- What are advantages, positive aspects and chances of online participation?
- What's the concrete benefit of online participation: for you personally? For others? For society?
- *→Laddering to assess and understand the „higher end states" (motivation and expectations)*
- What are the disadvantages, negative aspects and risks of online participation?

Correspondence to:
Christian Pieter Hoffmann
University of Leipzig
Institute of Communication and Media Studies
Burgstrasse 21
DE-04109 Leipzig

Email: christian.hoffmann(at)uni-leipzig.de

About authors

Christian Pieter Hoffmann is professor of communication management at the Institute of Communication and Media Studies, University of Leipzig. His research is focused on online communication, trust, self-disclosure and privacy protection in social media.

Christoph Lutz is an assistant professor at BI Norwegian Business School Oslo and research associate at the University of Leipzig. His dissertation focused on online participation. Further research interests include social media use in science and public administration, online privacy and trust, and digital serendipity.

Giulia Ranzini is an assistant professor at the Department for Communication Science at the VU Amsterdam. Her research interests include social media, online identities, online dating and gender-related questions in computer-mediated communication.