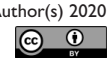
Article

new media & society
2020, Vol. 22(7) 1168–1187



DOI: 10.1177/1461444820912544
journals.sagepub.com/home/nms


Data capitalism and the user: An exploration of privacy cynicism in Germany

Christoph Lutz
BI Norwegian Business School, Norway

Christian Pieter Hoffmann
University of Leipzig, Germany

Giulia Ranzini
Vrije Universiteit Amsterdam, Netherlands

Abstract

Ever since empirical studies found only a weak, if any, relationship between privacy concerns and privacy behavior, scholars have struggled to explain the so-called privacy paradox. Today, a number of theoretical arguments illuminate users' privacy rationales, including the privacy calculus, privacy literacy, and contextual differentiations. A recent approach focuses on user resignation, apathy, or fatigue. In this piece, we concentrate on privacy cynicism, an attitude of uncertainty, powerlessness, mistrust, and resignation toward data handling by online services that renders privacy protection subjectively futile. We discuss privacy cynicism in the context of data capitalism, as a coping mechanism to address the tension between digital inclusion and a desire for privacy. Moreover, we introduce a measure for privacy cynicism and investigate the phenomenon based on a large-scale survey in Germany. The analysis highlights the multidimensionality of the construct, differentiating its relationships with privacy concerns, threat experience, Internet skills, and protection behavior.

Keywords

Online privacy, privacy concerns, privacy cynicism, privacy paradox, survey

Corresponding author:
Christoph Lutz, Nordic Centre for Internet and Society, BI Norwegian Business School, Nydalsveien 37, Oslo 0484, Norway.
Email: christoph.lutz@bi.no

Introduction

The degree to which the social is intertwined with the Internet in the digital age is nicely encapsulated by the concept of "digital citizenship." Mossberger et al. (2008) define digital citizenship as "the ability to participate in society online" and frame it as a prerequisite for social inclusion (p. 1). This perspective aligns with research on digital inequalities, which highlights the exclusionary implications of lacking access to digital media and failing to participate online (DiMaggio et al., 2001). Proponents of the digital citizenship concept argue that citizens need to be educated in "safe and responsible behavior online" (Jones and Mitchell, 2016: 2064), so that they refrain from risky practices, such as sexting, and avoid falling prey to abusive behavior, such as cyberbullying. However, for most users, participation in society online is associated with risks, such as online harassment, spam, hacking, or identity theft (Blank and Lutz, 2018; Dodel and Mesch, 2018).

Academic literature has long investigated such phenomena within the field of online privacy. On the one hand, threats to the integrity of users' personal data are likely to affect their social, economic, and mental well-being. On the other hand, digital participation is impossible without sharing personal data (Ellison et al., 2007; Kane et al., 2014; Krasnova et al., 2010). Previous attempts to theorize information sharing, such as Communication Privacy Management theory, have argued that users are often aware that by sharing their information they extend its ownership to their audience (Petronio, 2002). However, with the expansion of social media and the ubiquitousness of mobile technology, users struggle with estimating the sizes and compositions of their online audiences (Litt, 2012). In addition, more recent and mobile-based social media platforms, like Instagram and Snapchat, include design principles aimed at promoting habitual use (Bayer et al., 2015), incentivizing users to share (Chen et al., 2017). As a result, and paradoxically, most Internet users report both high levels of privacy concerns and high levels of private information disclosure, while abstaining from rigorous privacy-protective behaviors (Young and Quan-Haase, 2013).

Recent reflections on "surveillance capitalism" (Zuboff, 2019) or "data capitalism" (West, 2019) highlight (a) the role of digital platforms as critical social infrastructures of modern society, imposing significant disadvantages on individuals who refrain from their usage, and (b) the extraction of personal data as a constitutive characteristic of digital platforms' business models. Such perspectives underline that individuals can no longer meaningfully participate in society without paying with their personal data as a kind of entrance fee. The so-called privacy paradox (Kokolakis, 2017), therefore, can be understood as an indicator of this new social reality, as platform users are concerned by the commodification of their data, yet continue to share personal data to achieve social inclusion.

The privacy calculus has emerged as the most prominent model to explain the privacy paradox, particularly in regard to institutional privacy threats (Raynes-Goldie, 2010; Young and Quan-Haase, 2013). According to this approach, users weigh the expected benefits from online transactions against the perceived risks. When the benefits override the risks, users will disclose personal information and the privacy paradox occurs (Dinev and Hart, 2006). However, the privacy calculus assumes that users act rationally and have full agency, which is often not realistic. More recent approaches in privacy research

attempt to more explicitly account for the complexity of privacy-related decision-making by arguing that many individuals have resorted to privacy fatigue, privacy cynicism, surveillance realism, or privacy apathy (Hoffmann et al., 2016; Choi et al., 2018; Dencik and Cable, 2017; Hargittai and Marwick, 2016). As a result, instead of adapting their behavior, users have developed coping mechanisms to manage the tension between online participation as a "digital citizen" and the risks deriving from digital platforms' access to personal data.

However, the mentioned studies on privacy fatigue, privacy cynicism, surveillance realism, and privacy apathy are, to this stage, mostly based on qualitative research and not strongly developed in conceptual terms. In this article, we provide more generalizable evidence on the phenomenon, discussing findings from a large-scale survey on online privacy in Germany. In particular, we test a nomological model of privacy cynicism. We show that powerlessness and mistrust are the most prevalent dimensions of privacy cynicism in Germany, while resignation is the least pronounced. Our findings contribute to the burgeoning online privacy literature (Baruh et al., 2017) and connect it to the growing debate around the surveillance economy and data capitalism. They also provide a quantitative approach to a theme of powerlessness experienced by Internet users when it comes to participating in the digital society. A key contribution is the differentiation of dimensions of privacy cynicism. As our analyses show, these dimensions have distinct effects on privacy protection and are associated with established constructs such as privacy concerns and Internet skills in different ways.

Literature review

The paradox of online privacy

Many fundamental privacy theories include, at their core, the notion of control. Westin's definition of privacy was grounded on individuals' self-determination of what to disclose and what to keep private (Westin, 2003; Westin and Ruebhausen, 1967). Altman (1977) claimed that individuals achieve their optimum level of privacy through a process "dependent on [their] ability to control interactions with others" (p. 67). Building on Altman's idea of privacy as a non-monotonic process, modern approaches have conceptualized privacy as contextual (Nissenbaum, 2004) or situational (Masur, 2018). Especially within Masur's (2018) situational approach, privacy is evaluated in each specific context, and control (through, for example, audience management) is put in place so that self-disclosure can take place. Taken in absolute terms, these approaches suggest that, as a response to a concerning privacy context, individuals would limit their self-disclosure. Yet several studies have found that, on the Internet, users reveal substantial amounts of sensitive personal data despite high privacy concerns. The concept of a "privacy paradox" (Barnes, 2006) describes discrepancies between privacy attitudes and behavior (Norberg et al., 2007). More recent research has determined a weak, if any, effect of privacy concerns on online self-disclosure and privacy protection (Dienlin and Trepte, 2015; Kokolakis, 2017).

However, the empirical evidence on the privacy paradox is mixed and many theoretical explanations have been attempted (Baruh et al., 2017; Kokolakis, 2017). According

to Kokolakis (2017), more studies find evidence in favor of the paradox than against it. Yet in a meta-analysis of 166 studies, Baruh et al. (2017) report that, on aggregate, privacy concerns have a small negative effect on the use of online services and a small positive effect on privacy protection behavior. Social network sites (SNS), however, stand out as the exception where a paradox between concerns and behavior is found (Baruh et al., 2017). This highlights how SNS might have become pieces of critical social infrastructure, where participation is unavoidable, and the balance between user privacy and inclusion is challenging to manage. The exceptional status of SNS in the meta-analysis also points to the importance of context in the study of online privacy (Nissenbaum, 2004). Particularly it is important to distinguish between institutional privacy threats, as posed by institutions such as platform providers, and social privacy threats that emanate "horizontally" from other users (Raynes-Goldie, 2010; Young and Quan-Haase, 2013). Previous research has shown that users react more strongly to social than institutional privacy threats (boyd and Hargittai, 2010), indicating a higher level of either indifference or helplessness when facing threats emanating "vertically" from institutions.

Scholars have developed different explanations for the absence of an effect of privacy concerns on user behavior. Among these, the *privacy calculus*, where users weigh the benefits of a transaction against its risks, has been the dominant approach (Dinev and Hart, 2006; see Kokolakis, 2017). Within a privacy calculus perspective, the decision to disclose information is strongly affected by individuals' perceptions of what is privacy invasive (Hurwitz, 2013). Criticisms to this approach have focused on its excessive reliance on human rationality (Keith et al., 2013) and lack of situational adaptability (Masur, 2018).

Another explanation for the privacy paradox focuses on a *lack of risk awareness* among users. Many users lack understanding of online privacy risks, for example, due to a lack of privacy literacy or Internet skills (Bartsch and Dienlin, 2016; Dienlin and Trepte, 2015). Previous research suggested a positive relationship between Internet skills and privacy protection (Büchi et al., 2017; Park, 2013). In the context of Facebook, for example, highly skilled users modify their privacy settings more frequently than less skilled users (boyd and Hargittai, 2010). Hence, Internet skills, or more specifically privacy literacy, might be a better predictor of privacy behavior than privacy concerns. Yet, privacy literacy tends to be low and its effect on (social) privacy behavior is weak or absent (Bartsch and Dienlin, 2016; Kezer et al., 2016).

In this study, we will advance our understanding of privacy by drawing on a newly developed concept that complements the available explanations for the privacy paradox: privacy cynicism. The concept of privacy cynicism describes users' attitude toward data protection and privacy, within a context of limited subjective agency (Hoffmann et al., 2016). Users report a feeling of powerlessness when faced with a complex and opaque online landscape, where platforms, institutions, and other users have unprecedented access to their data (Hoffmann et al., 2016). This feeling of digital resignation (Draper and Turow, 2019), particularly when faced with institutional privacy threats, has also been addressed under the terms privacy apathy (Hargittai and Marwick, 2016), privacy fatigue (Choi et al., 2018), and surveillance realism (Dencik and Cable, 2017). In the next two sections, we will discuss current perspectives on surveillance capitalism (Zuboff, 2019) and data capitalism (West, 2019) and then, informed by these critical accounts, review

conceptualizations of user powerlessness in the form of surveillance realism, privacy apathy, and privacy fatigue. Finally, we will present privacy cynicism as our take on the topic and derive the hypotheses for our research model.

Data capitalism: challenges to user agency

The first definition of the Internet as a Panopticon was formulated by Campbell and Carlson as early as 2002. Drawing upon Foucault, the authors observe how consumerism leads users to share private information "in the belief that [they] will ultimately benefit from such disclosure through convenient access to goods and or services" (Campbell and Carlson, 2002: 592). In the last decade, data collection by online platforms has increased in comprehensiveness as algorithms rely on behavioral data to adapt and expand online services. This has generated a system of data capitalism, where the surveillance of users generates value (West, 2019). According to Zuboff, these personal data are both made necessary for users to access services, and endlessly monetizable for the platforms collecting it, analyzing it, and selling it to third parties (Zuboff, 2019).

A common thread in the surveillance capitalism or data capitalism critique of digital platforms is their challenge to user agency. Referencing Mark Zuckerberg's description of SNS as "social infrastructure", West (2019) highlights that "[u]sers are placed in a double bind, caught between desires for privacy and the ability to form meaningful communities with other users online without opting out of these services." (p. 37)

Hence, the challenge to user agency in relation to data protection becomes vastly more complicated in the context of social media platforms. Several studies highlighted how, without a sufficient level of self-disclosure, users will find it hard to establish social connections (boyd, 2007; Kane et al., 2014). Social media platforms eagerly frame self-disclosure as a contribution to the community, repaid by the self-disclosure of other members (Ellison et al., 2007). Recent critics, however, point out that, thanks to the harvesting of behavioral data, platforms might have eroded users' choice not to share personal data (West, 2019; Zuboff, 2019). This might reflect in a disconnect between individuals' abstract concept of what privacy should be, and what they obtain while participating on the platforms (Sujon, 2018).

New perspectives: surveillance realism, privacy apathy, and privacy fatigue

Dencik and Cable's (2017) concept of *surveillance realism* tackles the relationship between privacy and disempowerment. Embedded in surveillance literature, their study was born out of the revelations about bulk data collection by Edward Snowden. Situated in the United Kingdom and based on qualitative research, the authors describe a general attitude of resignation regarding institutional data practices. This attitude is termed surveillance realism and defined as "a simultaneous unease among citizens with data collection alongside the active normalization of surveillance that limits the possibilities of enacting modes of citizenship and of imagining alternatives" (Dencik and Cable, 2017: 763). Surveillance realism is inspired by the notion of "capitalism realism" (Fisher, 2009), which describes the attitude of people being so accustomed to capitalism that they could not imagine alternative economic systems. In the study results, the authors

highlight a lack of behavioral changes in the face of institutional privacy threats, pointing to user resignation, self-censorship, and a "general sense of disempowerment" (p. 775). Surveillance realism is, however, strongly tied to state surveillance, and is not easily applicable to corporate surveillance or social privacy.

Hargittai and Marwick (2016) introduce the concept of *privacy apathy* to address the lack of privacy protection behavior among users in the United States. Using focus groups and survey data, participants acknowledged the networked nature of online privacy (Marwick and boyd, 2014), including a lack of control over personal data and issues of passive participation (Lutz and Hoffmann, 2017). After addressing privacy protection strategies, the authors briefly discuss "apathy and cynicism" (pp. 3751–3752). Specifically, resignation about privacy violations is mentioned as an expression of apathy. Similar to Dencik and Cable (2017), the authors identify resignation as a response to the lack of conceivable alternatives to the current surveillance landscape. Despite being cynical, the participants still try to protect their privacy, so that the overall attitude toward privacy, in line with Turow et al. (2015) as well as Draper and Turow (2019), is described as "resigned pragmatism" (Hargittai and Marwick, 2016: 3752).

Choi et al. (2018) develop the concept of *privacy fatigue* as "the sense of weariness toward privacy issues, in which individuals believe that there is no effective means of managing their personal information on the Internet" (p. 42). The authors contextualize privacy fatigue within recent data breaches. Theoretically, the study is embedded in psychological literature on fatigue, which describes an unpleasant form of exhaustion resulting from high expectations and the inability to meet these demands. The authors define privacy fatigue as a negative coping mechanism, where individuals become disengaged and fail to protect themselves. Cynicism is seen as a core component of privacy fatigue. In the results of their survey-based study, conducted in South Korea, the authors find that privacy fatigue has a positive effect on the intention to disclose personal information and on disengagement, whereas privacy concerns have a negative effect.

While surveillance realism, privacy apathy, and privacy fatigue present important steps toward understanding how citizens try to resolve the tension between social inclusion and privacy online, they come with at least two shortcomings. First, the studies are based on small and specialized samples, making generalizations problematic. Second, the concepts largely neglect previous research and theories in other fields that could help structure the phenomenon (as an exception, see Draper and Turow, 2019). To address these limitations, we propose privacy cynicism as a related and suitable concept. It is motivated by social psychology and tested through more generalizable data. In the following, we discuss the concept of privacy cynicism and embed it into a nomological model with related constructs such as privacy concerns, Internet skills, and privacy threat experience.

Privacy cynicism

The concept of privacy cynicism was developed to help in our understanding of the privacy paradox, particularly in the context of institutional privacy threats (Hoffmann et al., 2016). It represents a cognitive coping mechanism, allowing users to overcome or ignore privacy concerns and engage in online transactions, without ramping up privacy protection efforts.

Cynicism has been explored primarily in dyadic relationships. It implies assumptions over the motives of an interaction partner (Mills and Keil, 2005), who is presumed to be driven by self-interest, and eager to take advantage of the person concerned. As trust is based on assumptions of competence, benevolence, and integrity (Bhattacherjee, 2002), cynicism implies a level of mistrust and antagonism (Almada et al., 1991).

Another important element associated with cynicism is a feeling of powerlessness. In dyadic relationships, when one of the two agents is left with little or no control over decision-making, they will be more likely to grow cynical about the other's motives and actions (Dean et al., 1998). Previous research has linked cynicism to outcomes such as lack of institutional trust and engagement (Langworthy, 1987), and repercussions for well-being, such as burnout (Salanova et al., 2005).

While cynicism has been defined as either an attitude or a belief (Andersson, 1996; Dean et al., 1998), it also functions as a coping mechanism. Individuals resort to cynicism when they are unable to control the circumstances behind their decision-making. In this context, risks are not discounted, but rather perceived as inevitable, because they are entirely out of their control (Kanter and Mirvis, 1989). This perception supports inaction in the face of potentially harmful circumstances and presents an interesting lens through which online self-disclosure and privacy threats can be approached. In a scenario such as data or surveillance capitalism, where users think they have limited control over their information, privacy protection might seem useless.

As such, we understand privacy cynicism as an attitude of uncertainty, powerlessness, and mistrust toward the handling of personal data by digital platforms, rendering privacy protection subjectively futile (Hoffmann et al., 2016). We argue that a system of data capitalism, based on the harvesting of private data, coupled with devices designed to maximize user interaction might have made situational evaluations of available privacy (Masur, 2018) too complicated for users to take into account when choosing their desired level of disclosure (Hoffmann et al., 2016). In this context of ubiquitous institutional privacy threats, privacy cynicism can be understood as a cognitive coping mechanism because it allows subjectively disempowered users to participate in online platforms without cognitive dissonance since they rationalize privacy protection as useless.

We expect privacy cynicism attitudes to be negatively related to Internet skills and privacy protection (Hoffmann et al., 2016; Park, 2013), as high-skilled users should feel less powerless vis-à-vis service providers. Previous research on privacy and Internet skills has found a positive and strong effect of Internet skills on privacy protection (Bartsch and Dienlin, 2016; Büchi et al., 2017; Masur, 2018). We argue that more skilled Internet users have higher agency when it comes to data protection and privacy online, which should result in lower levels of disempowerment and thus cynicism. Therefore, our first hypothesis introduces an association between Internet skills and privacy cynicism:

H1. Internet skills and privacy cynicism are negatively associated.

Compared with Internet skills, privacy threat experience is more closely tied to specific security risks that occur online such as spam, hacking, and phishing. We argue that privacy threat experience and privacy cynicism are generally positively associated.

Threat experience is likely to bolster mistrust in service providers. Particularly under conditions of uncertainty, threat experiences may also induce feelings of powerlessness and, ultimately, resignation. However, if users experience little uncertainty or high levels of efficacy, threat experiences could also lead to more protection behavior rather than resignation. So the relationship of threat experience and cynicism is likely to be moderated. For the sake of clarity, our model will not delve into such moderation effects, and given low privacy literacy among large segments of Internet users (Bartsch and Dienlin, 2016), we propose a net positive effect:

H2. Privacy threat experience and privacy cynicism are positively associated.

Privacy concerns are a key construct in privacy research. Their interrelation with privacy protection behavior and online self-disclosure is at the heart of the privacy paradox literature (Baruh et al., 2017; Kokolakis, 2017). Privacy concerns go beyond awareness and experience by capturing worries. We argue that such concerns are connected to cynicism, especially if user agency is perceived to be diminished (powerlessness). Higher levels of privacy concerns are associated with higher levels of attention to privacy issues, specifically privacy threats. As a result, feelings of mistrust and uncertainty should be related to privacy concerns:

H3. Privacy concerns and privacy cynicism are positively associated.

The first three hypotheses focus on privacy cynicism as a dependent construct; however, within our nomological model, privacy cynicism also serves as an independent construct: We argue that privacy cynicism and privacy protection behavior are associated. Cynicism, especially in a strong sense of powerlessness and resignation, renders privacy protection behavior subjectively futile (Hoffmann et al., 2016). Choi et al. (2018) tested this effect for privacy fatigue and found a positive and significant effect on disclosure intention. Since privacy protection behavior is an attempt to limit disclosure and keep certain information non-accessed, requiring cognitive effort, we propose that privacy cynicism will inhibit such activity:

H4. Privacy cynicism and privacy protection behavior are negatively associated.

While the relationship between privacy concerns and privacy protection behavior lies at the heart of the privacy paradox discussion, based on the latest empirical findings, we hypothesize a positive relationship (Baruh et al., 2017; Kokolakis, 2017):

H5. Privacy concerns and privacy protection behavior are positively associated.

Privacy threat experience and privacy concerns are related but conceptually distinct constructs. Given their similarity, we suggest that there should be a positive relationship between the two. More specifically, users with higher levels of privacy threat experience will likely be more concerned, as privacy risks are more visible and tangible to them:

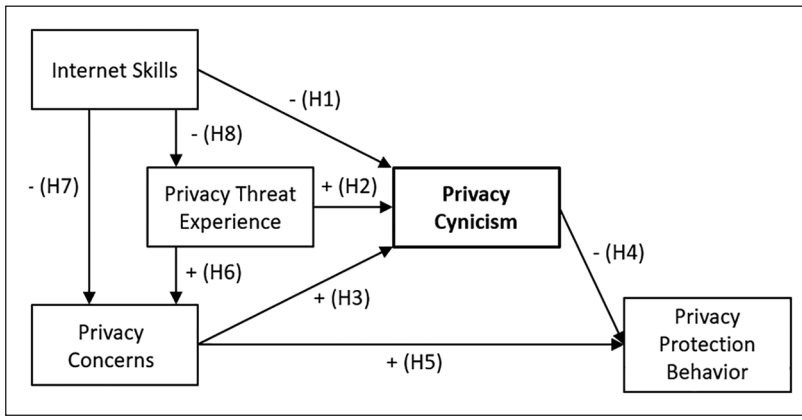


Figure 1. Research model.

H6. Privacy threat experience and privacy concerns are positively associated.

Internet skills could help assess online privacy in a more nuanced and fact-based way. By doing so, Internet skills could alleviate unfounded concerns. Highly skilled Internet users can be expected to perceive higher levels of efficacy and control, rendering them less vulnerable to privacy threats. We therefore propose a negative relationship between Internet skills and privacy concerns:

H7. Internet skills and privacy concerns are negatively associated.

Finally, we a postulate a negative association between Internet skills and privacy threat experience. Internet skills imply the ability to proactively use the Internet in different ways. Such skills, while largely implicit, also entail specific knowledge on the more explicit side, for example, in terms of security and privacy, which can protect against privacy threat experience:

H8. Internet skills and privacy threat experience are negatively associated.

Figure 1 shows the overall model. In the following, we first explore the dimensionality of privacy cynicism before testing the nomological model developed.

Methods

Data

We used data collected through an online survey in Germany between November and early December 2017. Access to the sample was provided by a certified market research institute. A total of 1008 respondents completed the survey. Gender and age quotas were applied to ensure a sample composition roughly equivalent to the overall German

population; 516 (51%) respondents reported being female and 492 (49%) being male. The average age in the sample was 50 years with a standard deviation (*SD*) of 18 years. The respondents were more educated than the German average, with 1% in our sample reporting no degree, 14% a lower secondary degree (*Volks- und Hauptschule*), 36% an intermediary secondary degree (*Mittlere Reife/Realschule*), 46% a higher secondary degree (*Fachhochschulreife oder Allgemeine Hochschulreife*), and the remaining 3% having missing values or reporting "Other." Participants were remunerated for completing the survey and received up to 50 cents. The median completion time was 704 seconds (about 12 minutes). The survey was based on a non-probability sample and the findings are therefore not representative of the general German population or Internet population. For example, we did not receive a specified confidence level and interval. Nevertheless, the wide age range allows broader generalizability than convenience and student samples.

Measures and method

To measure privacy cynicism, we developed an original scale based on previous conceptual work and qualitative studies as well as a number of small-scale quantitative student surveys. Ultimately, 27 items relating to privacy cynicism were included, all measured on 1–5 Likert-type scales (1 = strongly disagree; 5 = strongly agree). Prior to the survey, we conducted two pilot student surveys in German ($N = 58$ and 120, respectively) to test initial versions of the instrument and refine the scales. Thus, the wording of the items underwent several rounds of iteration. Feedback from English native speakers was collected for the English translation of the final items. The items were geared toward Internet services such as Google and Facebook. In an initial exploratory factor analysis (principal axis factoring extraction, promax rotation, Kaiser criterion in SPSS, v. 25), the dimensionality of privacy cynicism was assessed. In this process, four items were removed, leaving us with a clear 23-item measurement for privacy cynicism and four dimensions (see discussion below). In the ensuing structural equation model (SEM; MPlus v. 7.11, robust maximum likelihood estimator MLR), we opted for the same dimensionality but with four items per construct for better model fit.

We measured privacy concerns with three items from Malhotra et al. (2004). Privacy protection behavior was measured with five items from Milne et al. (2004) as well as Youn (2009). Privacy threat experience was measured with three items from a set of items developed by the authors based on commercial polls on privacy issues in Germany. Internet skills were measured with seven (out of 30) items from Hargittai's (2009) scale, which queries respondents for their knowledge of Internet and computer terms. Respondents had to indicate their level of understanding of these terms using a 5-point scale that ranged from 1 = no understanding to 5 = full understanding. We had included one bogus item for control (proxypod) that was not used in the SEM. All six remaining items loaded neatly on one factor and revealed high internal consistency (Cronbach's $\alpha = .90$). Due to the relatively high correlation between pdf and advanced search and lower loading than the other four items, we dropped these two items in the SEM, leaving us with a four-item measurement for Internet skills (spyware, wiki, phishing, cache).

All constructs had good internal consistency and convergent validity, except for privacy protection behavior and privacy threat experience, which proved to be problematic

in terms of the factor loadings. Nevertheless, we retained the constructs due to their importance in the overall model and the lack of a more established alternative. Based on the Fornell–Larcker test, discriminant validity can be assumed (Fornell and Larcker, 1981). The wording of the constructs used is displayed in Supplemental Appendix A, the measurement in Supplemental Appendix B, and the discriminant validity test in Supplemental Appendix C. Due to high correlation of the error term between the second and third privacy protection item (potentially due to similar question wording, starting with "Asking a website . . ." and resulting in a modification index of 243.131), we allowed the covariance between the error terms of these items to be freely estimated.

Results

Descriptive statistics and dimensionality

The four factors comprising the dimensions of privacy cynicism are: mistrust (seven items), uncertainty (six items), powerlessness (five items), and resignation (five items) (Table 1). All components displayed high internal consistency and the overall solution had very good sampling adequacy, as seen in the high Kaiser–Meyer–Olkin (KMO) value of .90 (Kaiser and Rice, 1974). Mistrust had an arithmetic mean across all items of 3.50 ($SD = 0.93$), uncertainty of 3.19 ($SD = 1.00$), powerlessness of 3.59 ($SD = 0.94$), and resignation of 2.46 ($SD = 1.08$). German users thus feel quite powerless and distrustful toward Internet companies, but not to a point where this is reflected in widespread resignation. The correlations between the privacy cynicism dimensions are all positive and statistically significant ($p = .000$) but moderate. They range from .42 between powerlessness and uncertainty to .20 between powerlessness and resignation.[1] Thus, the dimensions are related but can be analyzed independently.

SEM

The SEM had good model fit, Chi-Square = 881.075 ($p = .000$), degrees of freedom (df) =407, root mean square error of approximation (RMSEA) = 0.037 (90% confidence interval [0.033, 0.041]), comparative fit index (CFI) = 0.953, Tucker–Lewis index (TLI) = 0.946; standardized root mean square residual (SRMR) = 0.048. We found support for H1 for three privacy cynicism dimensions (Table 2), as Internet skills have a significant negative effect on uncertainty, powerlessness, and resignation. Thus, Internet skills mitigate privacy cynicism but they do not counteract mistrust in Internet companies. Equally, we found support for H2 for three privacy cynicism dimensions: Privacy threat experience affects uncertainty, powerlessness, and resignation positively. Thus, the higher the users' privacy threat experience, the more cynical they tend to be. Interestingly, we found no significant effect for the first privacy cynicism dimension of mistrust, so mistrust in services does not appear to be driven by firsthand experience. Turning to H3, we again found support for three privacy cynicism dimensions (Table 2). Privacy concerns increase elements of privacy cynicism in the form of mistrust, uncertainty, and powerlessness. However, for resignation, the effect is negative. Thus, the more concerned users are, the less they are resigned, indicating that concern has a nuanced effect on cynicism.

Table 1. Exploratory factor analysis.

Factor number and name	Items	Loading	α
1: Mistrust	I think that Internet companies are unreliable.	0.875	0.908
	Internet companies can't be trusted.	0.871	
	I think that Internet companies are not honest.	0.848	
	I think that Internet companies don't have my best interests in mind.	0.826	
	In the end, Internet companies only want to make money with our data.	0.691	
	Large Internet companies do with our data what they want.	0.619	
	I assume that Internet companies are only interested in their own benefit but not in mine.	0.501	
2: Uncertainty	It is difficult to keep up-to-date with the many things that happen online.	0.808	0.895
	I am uncertain about what happens with my personal data on the Internet.	0.800	
	I am uncertain about what the services I use do with my personal data.	0.784	
	I am not sure if I do everything right when I use the Internet.	0.755	
	It is difficult to understand all the risks of using the Internet.	0.749	
	I am uncertain about what the other users I encounter online do with my personal data.	0.682	
3: Powerlessness	Even if I try to protect my data, I can't prevent others from accessing them.	0.815	0.869
	In the end, I can't prevent others from accessing my data.	0.747	
	I don't have the power to protect my personal data effectively from all the possible dangers on the Internet.	0.738	
	It would be naïve to think that I can protect my personal data online reliably.	0.736	
	If someone is determined to access my personal data, there is nothing I can do to stop them.	0.700	
4: Resignation	There is no point in dedicating too much attention to the protection of my personal data online.	0.877	0.859
	I can't be bothered to spend much time on data protection on the Internet.	0.776	
	I have given up trying to keep up-to-date with current solutions for protecting my personal data online.	0.707	
	I am careless with my personal data online because it is impossible to protect them effectively.	0.695	
	It doesn't make a difference whether I try to protect my personal data online or not.	0.617	

Table 2. Structural equation model for privacy cynicism dimensions.

DV: Mistrust		
Privacy concerns	0.360 (0.044)	.000
Privacy threat experience	0.091 (0.054)	.093
Internet skills	−0.021 (0.042)	.615
$R^2 = .155$		
DV: Uncertainty		
Privacy concerns	0.230 (0.047)	.000
Privacy threat experience	0.380 (0.048)	.000
Internet skills	−0.336 (0.040)	.000
$R^2 = .273$		
DV: Powerlessness		
Privacy concerns	0.128 (0.045)	.005
Privacy threat experience	0.289 (0.051)	.000
Internet skills	−0.174 (0.042)	.000
$R^2 = .120$		
DV: Resignation		
Privacy concerns	−0.185 (0.050)	.000
Privacy threat experience	0.184 (0.057)	.001
Internet skills	−0.256 (0.043)	.000
$R^2 = .094$		

DV: dependent variable.
Column 1: not bold: independent variables, Column 2: standardized path coefficients (standard errors), Column 3: *p* value.

Table 3. Structural equation model for privacy protection behavior.

DV: privacy protection behavior		
Privacy concerns	0.421 (0.059)	.000
Mistrust	0.223 (0.052)	.000
Uncertainty	0.092 (0.054)	.086
Powerlessness	−0.073 (0.052)	.159
Resignation	−0.167 (0.047)	.000
$R^2 = .350$		

DV: dependent variable.
Column 1: not bold: independent variables, Column 2: standardized path coefficients (standard errors), Column 3: *p* value.

Table 3 shows the result for hypotheses related to privacy protection behavior (H4 and H5). Our findings reveal a mixed picture and weak support for H4. Only one of the cynicism dimensions has the expected effect, namely resignation. Individuals who are more resigned protect their privacy less. Mistrust is significant but positive. Thus, users who have high levels of mistrust in Internet companies protect themselves more. The two remaining dimensions of uncertainty and powerlessness are insignificant. H5 is supported, as privacy concerns have a positive and pronounced effect on privacy protection behavior. Thus, we find no evidence for the privacy paradox in our model.

Table 4. Structural equation model for privacy concerns and privacy risk awareness.

DV: privacy concerns		
Privacy threat experience	0.287 (0.058)	.000
Internet skills	−0.028 (0.047)	.558
$R^2 = .079$		
DV: privacy threat experience		
Internet skills	0.279 (0.045)	.000
$R^2 = .078$		

DV: dependent variable.
Column 1: not bold: independent variables, Column 2: standardized path coefficients (standard errors), Column 3: *p* value.

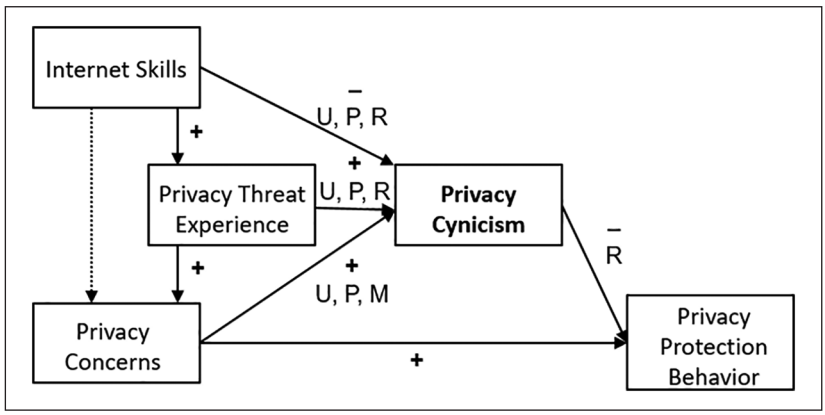


Figure 2. Summary of SEM results.
M: Mistrust; U: Uncertainty; P: Powerlessness; R: Resignation; dotted arrow: insignificant relationship; straight arrow: significant relationship; +: positive relationship; –: negative relationship.

Table 4 shows the results for the remaining hypotheses. We find support for H6 as privacy threat experience has the expected positive effect on privacy concerns. Internet skills and privacy concerns, by contrast, are not significantly associated (H7). Finally, Internet skills have a positive and significant effect on privacy threat experience, rather than the predicted negative effect. Thus, H8 is rejected.

Figure 2 provides an overview of the hypotheses. Five of eight hypotheses are supported or mostly supported, while three hypotheses are rejected or partially rejected. Most variance could be explained for privacy protection behavior (Table 3). Among the privacy cynicism dimensions, uncertainty can be best explained with the three predictor constructs (Table 2), with an explained variance of 27%, followed by mistrust (16%), powerlessness (12%), and resignation (9%).

Discussion and conclusion

As digital platforms, and social media in particular, emerge as "social infrastructures" of the digital age, research focuses on the evolving preconditions for participation and

inclusion (Blank and Lutz, 2018; Micheli, 2016; Van Deursen et al., 2017). Users' self-disclosure is one such precondition (Kane et al., 2014), and social media platforms are eager to frame the act of sharing as a contribution to the member community (Ellison et al., 2007; West, 2019). This is facilitated by the fact that, especially online, intimacy in relationships requires more extensive self-disclosure (boyd, 2006, 2007; Vitak, 2012). In addition, as the concept of digital citizenship (Mossberger et al., 2008) indicates, an argument can be made for the importance of digital platforms in the promotion of participation in society and social inclusion. However, the evolution of digital platforms into critical infrastructures comes at a high cost for user agency. Individuals face severe disbenefits if they refrain from the use of digital platforms (West, 2019; Zuboff, 2019). With social media platforms, such disbenefits combine the loss of personalized offers with the depletion of an important source of connection, resulting in social isolation, exclusion, or ostracism.

As highlighted by analyses of data capitalism (West, 2019) and surveillance capitalism (Zuboff, 2019), convenience as well as fundamental relational needs might lead individuals to feel "trapped" in the role of platform users. This can lead to disempowerment, hopelessness, and resignation when it comes to data protection. This development sheds new light on research addressing the so-called privacy paradox, especially in the context of institutional privacy concerns, by questioning assumptions of user rationality and agency. Recent studies have introduced concepts such as surveillance realism (Dencik and Cable, 2017), privacy apathy (Hargittai and Marwick, 2016), privacy fatigue (Choi et al., 2018), digital resignation (Draper and Turow, 2019), and privacy cynicism (Hoffmann et al., 2016). The latter concept was first derived from a review of cynicism literature and substantiated based on qualitative focus group data (Hoffmann et al., 2016). This article presents a preliminary measure of privacy cynicism, taking the multidimensionality of the concept into account. Our empirical analysis, based on a large-scale survey of Internet users in Germany, is the first to contribute quantitative empirical evidence to an emergent stream of online privacy research.

Our findings highlight the multidimensionality of privacy cynicism: *mistrust* describing the lack of faith in Internet companies, *uncertainty* describing the lack of knowledge and control about personal data online, *powerlessness* describing users' incapability of protecting themselves against potential harms to their data, and *resignation* describing the belief that privacy-protecting behaviors online are useless. While resignation, in particular, has been associated with cynicism and privacy apathy (Dencik and Cable, 2017; Draper and Turow, 2019; Hargittai and Marwick, 2016), it scores as the least prevalent factor. Resignation also behaves differently in relation to privacy concerns and privacy protection behavior. In particular, privacy concerns are negatively related to resignation, and resignation is negatively related to protection behavior. While resignation is the least pronounced component of privacy cynicism, it is still an interesting component to consider because it is—univocally—capable of preventing users to act on their concerns. However, the limited prevalence of resignation and the negative association with privacy concerns suggest that, while respondents might still feel that their ability to defend themselves against data misuse is limited, they do not perceive such an effort to be entirely useless.

This also speaks to the understanding of privacy as contextual (Nissenbaum, 2004) and situational (Masur, 2018) as users may not perceive the same level of resignation in

all settings and situations. As users are exposed to both vertical (i.e. institution-based) and horizontal (i.e. peer-generated) threats, they might perceive the latter as more worrying and worthy of their active attention (Sujon, 2018; Young and Quan-Haase, 2013). Accordingly, resignation may be less of a trait and more of a state. It should be noted, however, that in a digital domain, vertical and horizontal pressures interact: mistrust toward a platform may impede social interactions, and conversely, social concerns may lead to adjustments in platform use.

Powerlessness emerges as the most prevalent dimension of privacy cynicism. For our respondents, lacking control over the sharing of personal data online appears as the most salient dimension of privacy cynicism. This finding is especially relevant to privacy research, which tends to assume user agency as informational self-determination (Westin and Ruebhausen, 1967; to a lesser degree Altman, 1977), an assumption that may have to be reconsidered in the context of surveillance capitalism. In contexts or situations characterized by powerlessness, users may resist, withdraw, or, in some instances, resign, rather than regulate their level of self-disclosure. Beyond privacy research, the centrality of powerlessness to the phenomenon of cynicism should be of note. Digital platforms offer affordances for participation and inclusion, implying a potential for empowerment. However, in a context of surveillance and data capitalism, this potential may well be trumped by mistrust and powerlessness in relation to those platforms ostensibly providing the infrastructure for participation and inclusion. This again highlights how institutional pressures affect social dynamics. Policies and design interventions aiming at reducing or avoiding cynicism should be borne with the idea of giving agency back to users (Pybus et al., 2015). Kennedy and Moss (2015) discuss user agency in the context of social media data mining and offer three avenues for more empowered users: greater public supervision and regulation of data mining; making the tools for data mining, including software and literacy, more broadly available to the public; and initiatives that engage the public and stimulate reflections on their data practices (e.g. through good data journalism such as the Guardian's Reading the Riots project). A multi-stakeholder approach, combining several or all of these avenues, could be a fruitful approach to tackle powerlessness.

Mistrust also appears as an important component of privacy cynicism, especially as it pertains to institutional privacy. Previous research has highlighted that trust plays a relevant role as an antecedent to users' information sharing (Krasnova et al., 2010), and that users are relatively untrusting toward Internet services such as SNS (Lutz and Strathoff, 2014; Kim et al., 2012). This study extends such findings by highlighting how widespread mistrust plays into users' feelings of privacy cynicism. Our results suggest that higher privacy concerns generate more mistrust, independent of skills and threat experience. Generally, mistrust can predict privacy protection behavior, which speaks for conceptualizing cynicism multidimensionally, as mistrust and resignation co-occur among cynical users when situations are characterized by uncertainty and powerlessness. Conversely, in a situation where users feel they lack control over their data, having trust in the organizations handling their data may partially compensate for their powerlessness.

Our study also aims to establish a quantitative approach to privacy cynicism and the larger emergent research stream focusing on privacy apathy, fatigue, or resignation in the context of "data capitalism" (Dencik and Cable, 2017; Hargittai and Marwick, 2016). The quantitative analysis allows for a differentiated understanding of distinct dimensions

of cynicism, their respective prevalence, and effects. As an initial quantitative study, this analysis begs for further conceptual work to refine the relationships between salient constructs in the literature. As a first quantitative attempt to test privacy cynicism, this article has several limitations. First, while privacy literacy was at the core of our model, we did not control for the intensity of platform use of our respondents, which could influence their experience of privacy cynicism. We also have no indication of the respondents' knowledge of the data leaks that took place in the last years, and whether this impacted their experience of cynicism. Recent developments in privacy research describe privacy as contextual (Nissenbaum, 2004) and situational (Masur, 2018). This study cannot fully delve into the role of privacy cynicism in distinct contexts and situations as it is based on a cross-sectional study examining privacy cynicism more broadly. Finally, while our non-probability sample offers a comparative structure to the German population, it is not representative. As such, the national generalizability of our results is limited. Future studies could (a) differentiate distinct platforms as critical social infrastructures, (b) distinguish social and institutional platform benefits as well as privacy threats, (c) delve deeper into antecedents of user agency, (d) examine the situational role of cynicism as a state, and (e) provide a more comprehensive overview of cynicism outcomes in terms of inclusion and well-being. Among the dimensions of cynicism, powerlessness, in particular, could be taken up in future research and investigated in relation to forced sociality and commodification of social capital in the vein of data capitalism or surveillance capitalism (West, 2019; Zuboff, 2019). As such, this article constitutes a further step in a young research stream, hoping to inspire future research.

Funding

The author(s) disclosed receipt of the following financial support for the research, authorship, and/or publication of this article: Christoph Lutz was generously funded by Research Council of Norway, grant agreements 275347 "Future Ways of Working in the Digital Economy" and 247725 "Fair Labor in the Digitized Economy", during the work on this article.

ORCID iD


Christoph Lutz https://orcid.org/0000-0003-4389-6006

Supplemental material

Supplemental material for this article is available online.

Note

1. The correlations are as follows: mistrust and uncertainty: .20; mistrust and powerlessness: .40; mistrust and resignation: .22; powerlessness and uncertainty: .42; powerlessness and resignation: .20 uncertainty and resignation: .28.

References

Almada SJ, Zonderman AB, Shekelle RB, et al. (1991) Neuroticism and cynicism and risk of death in middle-aged men. *Psychosomatic Medicine* 53: 165–175.

Altman I (1977) Privacy regulation: culturally universal or culturally specific? *Journal of Social Issues* 33(3): 66–84.

Andersson LM (1996) Employee cynicism: an examination using a contract violation framework. *Human Relations* 49(11): 1395–1418.
Barnes SB (2006) A privacy paradox: social networking in the United States. *First Monday* 11(9).
Bartsch M and Dienlin T (2016) Control your Facebook: an analysis of online privacy literacy. *Computers in Human Behavior* 56: 147–154.
Baruh L, Secinti E and Cemalcilar Z (2017) Online privacy concerns and privacy management: a meta-analytical review. *Journal of Communication* 67(1): 26–53.
Bayer JB, Campbell SW and Ling R (2015) Connection cues: activating the norms and habits of social connectedness. *Communication Theory* 26(2): 128–149.
Bhattacherjee A (2002) Individual trust in online firms. *Journal of Management Information Systems* 19(1): 211–241.
Blank G and Lutz C (2018) Benefits and harms from Internet use: a differentiated analysis of Great Britain. *New Media & Society* 20(2): 618–640.
boyd d (2006) Friends, Friendsters, and MySpace Top 8: writing community into being on social network site. *First Monday* 11(12). Available at: https://journals.uic.edu/ojs/index.php/fm/article/view/1418/1336
boyd d (2007) Why youth ♥ social network sites. *MacArthur Foundation*. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1518924
boyd d and Hargittai E (2010) Facebook privacy settings: who cares? *First Monday* 15(8). Available at: https://firstmonday.org/article/view/3086/2589
Büchi M, Just N and Latzer M (2017) Caring is not enough: the importance of Internet skills for online privacy protection. *Information, Communication & Society* 20(8): 1261–1278.
Campbell JE and Carlson M (2002) Panopticon.com: online surveillance and the commodification of privacy. *Journal of Broadcasting & Electronic Media* 46(4): 586–606.
Chen T, Chen Y and Luo J (2017) A selfie is worth a thousand words: mining personal patterns behind user selfie-posting behaviours. In: *Proceedings of the 26th international conference on world wide web companion*, pp. 23–31. Geneva: International WWW Conferences Steering Committee. Available at: https://dl.acm.org/doi/abs/10.1145/3041021.3054142
Choi H, Park J and Jung Y (2018) The role of privacy fatigue in online privacy behavior. *Computers in Human Behavior* 81: 42–51.
Dean JW, Brandes P and Dharwadkar R (1998) Organizational cynicism. *Academy of Management Review* 23: 341–352.
Dencik L and Cable J (2017) The advent of surveillance realism. *International Journal of Communication* 11: 763–781.
Dienlin T and Trepte S (2015) Is the privacy paradox a relic of the past? *European Journal of Social Psychology* 45(3): 285–297.
DiMaggio P, Hargittai E, Neuman WR, et al. (2001) Social implications of the Internet. *Annual Review of Sociology* 27(1): 307–336.
Dinev T and Hart P (2006) An extended privacy calculus model for e-commerce transactions. *Information Systems Research* 17(1): 61–80.
Dodel M and Mesch G (2018) Inequality in digital skills and the adoption of online safety behaviors. *Information, Communication & Society* 21(5): 712–728.
Draper NA and Turow J (2019) The corporate cultivation of digital resignation. *New Media & Society* 21(8): 1824–1839.
Ellison NB, Steinfield C and Lampe C (2007) The benefits of Facebook "friends." *Journal of Computer-Mediated Communication* 12(4): 1143–1168.
Fisher M (2009) *Capitalist Realism*. Hants: Zero Books.
Fornell C and Larcker DF (1981) Evaluating structural equation models with unobservable variables and measurement error. *Journal of Marketing Research* 18(1): 39–50.

Hargittai E (2009) An update on survey measures of web-oriented digital literacy. *Social Science Computer Review* 27(1): 130–137.

Hargittai E and Marwick A (2016) "What can I really do?" Explaining the privacy paradox with online apathy. *International Journal of Communication* 10: 3737–3757.

Hoffmann CP, Lutz C and Ranzini G (2016) Privacy cynicism: a new approach to the privacy paradox. *Cyberpsychology: Journal of Psychosocial Resarch on Cyberspace* 10(4). Available at: https://cyberpsychology.eu/article/view/6280/5888

Hurwitz JB (2013) User choice, privacy sensitivity, and acceptance of personal information collection. In: Gutwirth S, Leenes R, De Hert P, et al. (eds) *European Data Protection: Coming of Age*. Dordrecht: Springer, pp. 295–312.

Jones LM and Mitchell KJ (2016) Defining and measuring youth digital citizenship. *New Media & Society* 18(9): 2063–2079.

Kaiser HF and Rice J (1974) Little Jiffy, Mark IV. *Educational and Psychological Measurement* 34: 111–117.

Kane GC, Alavi M, Labianca GJ, et al. (2014) What's different about social media networks? A framework and research agenda. *MIS Quarterly* 38(1): 275–304.

Kanter DL and Mirvis PH (1989) *The Cynical Americans: Living and Working in an Age of Discontent and Disillusion*. San Francisco, CA: Jossey-Bass.

Keith MJ, Thompson SC, Hale J, et al. (2013) Information disclosure on mobile devices. *International Journal of Human-Computer Studies* 71(12): 1163–1173.

Kennedy H and Moss G (2015) Known or knowing publics? Social media data mining and the question of public agency. *Big Data & Society* 2(2): 2053951715611145. Available at: https://journals.sagepub.com/doi/full/10.1177/2053951715611145

Kezer M, Sevi B, Cemalcilar Z, et al. (2016) Age differences in privacy attitudes, literacy and privacy management on Facebook. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace* 10(1): 2.

Kim HW, Xu Y and Gupta S (2012) Which is more important in Internet shopping, perceived price or trust? *Electronic Commerce Research and Applications* 11(3): 241–252.

Kokolakis S (2017) Privacy attitudes and privacy behaviour: a review of current research on the privacy paradox phenomenon. *Computers & Security* 64: 122–134.

Krasnova H, Spiekermann S, Koroleva K, et al. (2010) Online social networks: why we disclose. *Journal of Information Technology* 25(2): 109–125.

Langworthy RH (1987) Police cynicism: what we know from the Niederhoffer scale. *Journal of Criminal Justice* 15(1): 17–35.

Litt E (2012) Knock, knock. Who's there? The imagined audience. *Journal of Broadcasting & Electronic Media* 56(3): 330–345.

Lutz C and Hoffmann CP (2017) The dark side of online participation: exploring non-, passive and negative participation. *Information, Communication & Society* 20(6): 876–897.

Lutz C and Strathoff P (2014) Privacy concerns and online behavior – Not so paradoxical after all? Viewing the privacy paradox through different theoretical lenses. *SSRN Electronic Journal*. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2425132

Malhotra NK, Kim SS and Agarwal J (2004) Internet users' information privacy concerns (IUIPC). *Information Systems Research* 15(4): 336–355.

Marwick AE and boyd d (2014) Networked privacy. *New Media & Society* 16(7): 1051–1067.

Masur P (2018) *Situational Privacy and Self-Disclosure*. Cham: Springer.

Micheli M (2016) Social networking sites and low-income teenagers. *Information, Communication & Society* 19(5): 565–581.

Mills CM and Keil FC (2005) The development of cynicism. *Psychological Science* 16: 385–390.

Milne GR, Rohm AJ and Bahl S (2004) Consumers' protection of online privacy and identity. *Journal of Consumer Affairs* 38(2): 217–232.

Mossberger K, Tolbert CJ and McNeal RS (2008) *Digital Citizenship*. Cambridge, MA: MIT Press.
Nissenbaum H (2004) Privacy as contextual integrity. *Washington Law Review* 79: 119–157.
Norberg PA, Horne DR and Horne DA (2007) The privacy paradox. *The Journal of Consumer Affairs* 41(1): 100–126.
Park YJ (2013) Digital literacy and privacy behavior online. *Communication Research* 40(2): 215–236.
Petronio S (2002) *Boundaries of Privacy: Dialectics of Disclosure*. New York: State University of New York Press.
Pybus J, Coté M and Blanke T (2015) Hacking the social life of big data. *Big Data & Society* 2(2): 1–10. Available at: https://journals.sagepub.com/doi/full/10.1177/2053951715616649
Raynes-Goldie K (2010) Aliases, creeping, and wall cleaning: understanding privacy in the age of Facebook. *First Monday* 15(1). Available at: https://firstmonday.org/ojs/index.php/fm/article/view/2775/2432
Salanova M, Llorens S, Garcia-Renedo M, et al. (2005) Toward a four-dimensional model of burnout. *Educational and Psychological Measurement* 65: 901–913.
Sujon Z (2018) The triumph of social privacy: understanding the privacy logics of sharing behaviors across social media. *International Journal of Communication* 12: 3751–3771.
Turow J, Hennessy M and Draper N (2015) The tradeoff fallacy: how marketers are misrepresenting American consumers and opening them up to exploitation. *SSRN Electronic Journal*. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2820060
Van Deursen A, Helsper E, Eynon R, et al. (2017) The compoundness and sequentiality of digital inequality. *International Journal of Communication* 11: 452–473.
Vitak J (2012) The impact of context collapse and privacy on social network site disclosures. *Journal of Broadcasting & Electronic Media* 56(4): 451–470.
West SM (2019) Data capitalism: redefining the logics of surveillance and privacy. *Business & Society* 58(1): 20–41.
Westin AF (2003) Social and political dimensions of privacy. *Journal of Social Issues* 59(2): 431–453.
Westin AF and Ruebhausen OM (1967) *Privacy and Freedom*. New York: Atheneum.
Youn S (2009) Determinants of online privacy concern and its influence on privacy protection behaviors among young adolescents. *Journal of Consumer Affairs* 43(3): 389–418.
Young AL and Quan-Haase A (2013) Privacy protection strategies on Facebook. *Information, Communication & Society* 16(4): 479–500.
Zuboff S (2019) *The Age of Surveillance Capitalism: The Fight for the Future at the New Frontier of Power*. New York: PublicAffairs.

Author biographies

Christoph Lutz is an associate professor at the Nordic Centre for Internet & Society, BI Norwegian Business School (Oslo). His research interests include online participation, privacy, the sharing economy, and social robots. Christoph has published widely in top-tier journals in this area such as *New Media & Society*, *Mobile Media & Communication*, *Information*, *Communication & Society*, *Social Media + Society*, and *International Journal of Communication*.

Christian Pieter Hoffmann is professor for communication management at the Institute of Communication and Media Studies, University of Leipzig. His research portfolio is focused on strategic communication, political communication, online participation, digital inequality and privacy.

Giulia Ranzini is assistant professor at the faculty of Communication Science, Vrije Universiteit Amsterdam. Her broader research interests focus on the influence of technology on individual identities, relationships, and society at large.