Article

SM+S
social media + society

Social Media + Society
July-September 2023: 1–12

DOI: 10.1177/20563051231182365
journals.sagepub.com/home/sms
Sage

How Subjective Norms Relate to Personal Privacy Regulation in Social Media: A Cross-National Approach

German Neubaum[1], Miriam Metzger[2], Nicole Krämer[1], and Elias Kyewski[3]

Abstract

The growing body of research on privacy documents cross-cultural differences in the way people manage their privacy in social media. Yet, cultural values do not provide a consistent account for these differences. Drawing on communication privacy management theory, this work argues that different governmental approaches of privacy regulation shape users' subjective norms in the form of perceived rules about how to manage personal and collective boundaries. These subjective privacy norms may better explain cross-national differences in people's online privacy behavior. We conducted a survey (N = 1,060) among Facebook users in two countries in which privacy regulation policies vary significantly: the United States and Germany. While US users self-disclose more than German users do, they also take more measures to protect their privacy on Facebook. US users perceive stronger norms to protect themselves than German users. These findings inform communication privacy management theory and the influence of privacy rules within and across national borders.

Keywords

privacy regulation, communication privacy management theory, subjective norms, cultural differences

The idea that culture plays a role in privacy was pioneered by Altman (1977), who argued that while privacy regulation is a process that is observable universally, the particular mechanisms involved in regulatory activities are culturally specific. Indeed, governments apply different regulatory approaches to protect their citizens' privacy in today's digital age. For instance, in the European Union (EU), laws such as the 2018 European General Data Protection Regulation (GDPR) offer sweeping protection to individual privacy by restricting any organization that collects or processes the data of EU citizens. By contrast, in the United States, there is no general, comprehensive federal data protection law that regulates personal data collection and use (e.g., Boyne, 2018). Personal data collection is instead based on piecemeal state laws that regulate specific types of data, such as medical or financial information, in specific contexts (e.g., Blanchette & Johnson, 2002). Differences in privacy policy might be attributable to cultural differences in how privacy and its protection is viewed: While the US system treats privacy as a commodity subjected to negotiations over property, the European system sees privacy as a fundamental human right (Dogruel & Jöckel, 2019). This leads to the question of whether individual citizens deal with their personal privacy regulation differently depending on their culture, or more specifically, their country of residence.

A good deal of privacy research has examined the question of how individuals protect their privacy in online communication and which psychological factors predict the extent to which they disclose or withdraw personal information in social media (Acquisti et al., 2015; Baruh et al., 2017; Chen, 2018; Dienlin & Trepte, 2015; Kokolakis, 2017; Metzger & Suh, 2017). While many suggested that these connections should be analyzed in light of its cultural context (e.g., Acquisti et al., 2015; Baruh et al., 2017; Cho et al., 2018), relatively few studies have addressed the influence of national culture on individuals' online privacy attitudes and behavior. Initial cross-cultural studies provided evidence that users' perceptions of privacy threats online and their privacy protective behavior vary depending on the culture users live in (Krasnova & Veltri, 2010; Trepte & Masur, 2016; Trepte

[1]University of Duisburg-Essen, Germany
[2]University of California, Santa Barbara, USA
[3]University of Applied Sciences, Germany

Corresponding Author:
German Neubaum, Psychological Processes of Education in Social Media, Department of Computer Science and Applied Cognitive Science, University of Duisburg-Essen, Forsthausweg 2, 47057 Duisburg, Germany.
Email: german.neubaum@uni-due.de

et al., 2017). Moreover, macro-level cultural differences in privacy management have been proposed by privacy theorists (e.g., Altman, 1977; Petronio, 2002; Westin, 1967). Yet, the *reasons* for cross-cultural variations are not well understood.

The present study contributes to a small but growing body of research that examines privacy protection behavior from a cross-cultural perspective by proposing a missing link—subjective norms—to explain the influence of national culture on how people manage their online privacy. To this end, this study examines a hitherto untested assumption of privacy rule foundations formulated by existing theory in the sense that national contexts and promoted privacy rules therein affect people's subjective norms of online privacy. We analyze social media users' personal privacy management and its prerequisites in two countries that are known to differ significantly both in how individual citizens and their governments regulate privacy in online communication (Dogruel & Jöckel, 2019; Krasnova & Veltri, 2010; Trepte & Masur, 2016): the United States and Germany. Given its popularity in both countries at the time of data collection, this work will focus on the social networking site (SNS) Facebook to investigate people's online privacy regulation.

The Role of Culture in Communication Privacy Management

Privacy has been proposed as an interpersonal negotiation process of regulating and controlling who gets access to one's personal information and when (Altman, 1975). Communication Privacy Management (CPM) theory proposes that human beings reach their desired state of privacy (on a continuum between concealing and revealing information) by employing a rule-based privacy management system (Petronio, 2002). Accordingly, individuals perceive information as private when they see themselves as owners of information having the ability to determine who can be co-owners of their personal information. This co-ownership is marked by boundaries within which private information can flow. Based on that premise, individuals develop personal and collective criteria to regulate these boundaries, that is, rules that dictate when ownership of information can be shared. Petronio (2002) argues that people acquire the foundations for privacy rules throughout their socialization in the sense that they learn preexisting rules that were set implicitly or explicitly by the social context (family, organization) and, at a larger scale, the culture they live in: "Each culture values privacy differently and the values we place on privacy influence the rules we have for managing our privacy boundaries. Someone from a different culture may invade our privacy because he or she follows different rules" (Petronio, 2002, pp. 40–41). Others similarly argue that the negotiation of boundaries between human beings is context-dependent and that the "rules people follow for managing privacy vary by situation, are learned over time, and are based on cultural, motivational, and purely situational criteria" (Acquisti et al., 2015, p. 511). The boundary management system is subjected to turbulence when privacy rules are violated, interpreted differently, or learned in dissimilar social or cultural contexts. While CPM theory has proved to be a useful theoretical framework to analyze privacy regulation in computer-mediated communication (Child & Petronio, 2011; Dienlin & Metzger, 2016; Petronio & Child, 2020), relatively few studies have used this theory to analyze cross-national differences in privacy management.

The Influence of National Context on Personal Privacy Management Online

Prior research has corroborated the notion that personal rules to manage online privacy are shaped and executed in different manners across different countries (Bellman et al., 2004; Budak et al., 2017; Trepte & Masur, 2016; Yang & Kang, 2015; Zhang et al., 2007). Most comparative studies of privacy have utilized the individualism–collectivism continuum (i.e., the extent to which societies prioritize personal over collectivistic gains or individual independence over collective goals; Hofstede, 1997) as an explanatory framework. But findings are mixed as to whether people from individualistic or collectivistic cultures are more concerned about privacy or are stricter in their privacy management (Cho et al., 2009; Liang et al., 2017; Rui & Stefanone, 2013; Trepte et al., 2017; Wang & Liu, 2019; Yang & Kang, 2015). The cross-cultural differences have been interpreted in light of different accounts such as users' personal calculus weighing perceived benefits and risks of disclosing personal information (Trepte et al., 2017) or varying levels of privacy concerns or trust in one's government (Vitak et al., 2022). Given this, it has been suggested that the political system of the national context and how privacy is regulated on a governmental level might better explain the influence of national culture on personal privacy management (Bellman et al., 2004; Dogruel & Jöckel, 2019; Vitak et al., 2022). Indeed, recent research has proposed that legislative norms, regulated by law, stipulate rules for what kind of privacy behavior is desirable and which actions are sanctioned by society (Trepte, 2020). Applying the logic of CPM theory, one could argue that government privacy regulation policies may cultivate how sensitive individuals become toward their own privacy, and that this is reflected in their privacy behavior.

The two countries examined in the present study offer considerable variation in this regard: Germany as a member of the EU regulates users' privacy and data protection through the GDPR law. This regulation emphasizes privacy as a basic human right and strengthens the control that individuals have over their personal data by requiring organizations to be more transparent about user data collection. By contrast, the United States has no overarching federal law protecting personal

data. US law affords federal agencies little power to limit privacy-invading behaviors of private companies, and no legal expectation of privacy exists for individuals when data are shared or transmitted online.

While these different privacy policy approaches of the United States and Germany can be partly explained by how laws are passed in those different contexts, recent research has argued that diverging privacy regulatory approaches by governments may be a reflection of different cultural views of privacy (Dogruel & Jöckel, 2019; see also Bellman et al., 2004). National differences in boundary management are detectable, for instance, when social media users express how sensitive they find personal information and how willing they would be to share it online: Trepte and Masur (2016) found that German social media users rated all types of personal information as more sensitive than American users. Germans were also more protective of their personal information by limiting the visibility of profile information, while US users perceived open profiles to be less risky than Germans. Corroborating this pattern, research has shown that US social media users tend to disclose more personal information online than do Germans (Krasnova & Veltri, 2010). Building on this evidence and the expected national differences, we first predict:

Hypothesis 1 (H1). SNS users in Germany disclose less information about themselves than SNS users in the United States.

Hypothesis 2 (H2). SNS users in Germany take more measures to protect their privacy than do SNS users in the United States.

The Explanatory Value of Norms for Personal Privacy Regulation

It is plausible to argue that government regulation of online privacy represents a manifestation of collective rules that are set in societies to manage privacy boundaries. That is, even if privacy rules are negotiated among individuals as an outcome of interpersonal interaction, the rules that are predefined by a society may offer a framework for this negotiation (Movius & Krup, 2009). According to Petronio (2002), privacy rules for interpersonal interaction are conveyed to individuals in the form of social norms. Social norms are defined as rules or standards that are understood and accepted by members of a group or a society (Cialdini & Trost, 1998). Social norms operate in groups that may vary in size and composition, for instance, at a level of country, local community, and referent groups such as friends or family (Shulman et al., 2017). In line with Petronio's conceptualization of privacy rules, social norms are presumed to emerge in social interactions, leading the individual to perceive which behaviors are expected in their social environment (i.e., "subjective norms"; Cialdini & Trost, 1998).

In daily life, individuals encounter different sources of normative information, and can attribute normative expectations to different stakeholders. In terms of online privacy norms, social media users observe their peers protecting their own or other people's privacy (e.g., by limiting visibility or the audience for posts), which signals the desirability of privacy protection (Lewis et al., 2008; Utz & Krämer, 2009). Besides peers as sources of normative information, individuals are exposed to news media that cover the shortcomings of data protection of social media services, and large-scale data breaches (Pleger et al., 2021). A comprehensive content analysis of German press coverage in 2014–2015 showed that across different news media, coverage of privacy is associated with a consensus that the level of privacy protection in digital technologies is generally low (von Pape et al., 2017), which may promote the normative belief that protecting one's personal information is desirable. At the same time, and potentially due to the legal frameworks for protecting citizen's privacy, individuals might also form the subjective norm that in one's country of residence, it is more or less expected to protect one's private information in online channels. Thus, various sources of normative information can shape social media users' subjective norms about online privacy, which in Petronio's terms contributes to the acquisition of the rule-based management system.

Empirical evidence has documented the predictive value of social privacy norms regarding actual privacy-related behavior. In two experiments, Spottswood and Hancock (2017) showed that when social media users encounter explicit cues of other social media users (a) disclosing less (compared with relatively higher rates of) personal information or (b) adopting stricter privacy settings (compared with open privacy settings), they disclose personal information less frequently and select stricter privacy settings. Users thus appeared to adhere to social norms signaled by explicit cues in their own privacy behavior. The authors explained this effect by the "bandwagon heuristic," assuming that social media users follow the simple rule of thumb "if other people think that something is good or safe, then I should too" (p. 56; see Masur et al., 2021 for similar results). These subjective norms and their behavioral correlates, in turn, may vary from country to country (Ur & Wang, 2013). A cross-national survey on privacy-related behavior indicated that perceived group norms referring to privacy had a stronger positive association with individuals' sense of online privacy control in China compared with the United States (Liu & Wang, 2018). Based on this finding, Petronio and Child (2020) suggest that privacy rules in social media communication, that is, norms for boundary management, are negotiated differently across national borders.

In the specific comparative scenario of Germany versus the United States, the present study examines whether the form of government regulation of privacy affects subjective norms about privacy protection. There are many reasons for

the different legal situations toward privacy protection in the EU and the United States. While there has been major public support for the regulations of technology companies in the United States (Vogels, 2021), the jurisdiction and ideologically polarized policymaking in the United States are barriers to enact protective laws (Napoli & Dwyer, 2018). Still, scholarly views claim that the EU public places a higher value on privacy as a human right than the United States, which might be the determining factor that led to the ultimate enactment of the GDPR in the EU giving users more control over their data (Dogruel & Jöckel, 2019; Hallinan et al., 2012). A reasonable hypothesis is that by considering privacy as a basic human right, as manifested in the GDPR, social norms to protect one's personal data are promoted and perceived as stronger in Germany than they are in the United States. In fact, it has been observed that it is not that cultural values directly shape people's privacy concerns but rather the particular national regulation does (Bellman et al., 2004). This is indicative that governmental regulation of privacy establishes a normative framework that should be reflected in users' privacy perceptions. Accordingly, we argue that people's perceptions of subjective norms will explain cross-national differences in people's disclosure and privacy protection behavior in SNSs:

Hypothesis 3 (H3). SNS users in Germany perceive stronger subjective norms to protect their online privacy than SNS users in the United States.

Hypothesis 4 (H4). Subjective norms to protect one's privacy explain the cross-national differences predicted in *H1* and *H2*.

The Relationship between Privacy Norms and Predictors of Privacy-Related Behavior

Synthesizing communication privacy management theory and current research on online privacy, this study further proposes that commonly accepted rules in the form of subjective norms also affect the psychological variables that have been identified as reliable predictors of privacy behavior online, that is, online privacy attitudes, perceived privacy risks, and online privacy self-efficacy. Previous research documented empirically that attitudes (i.e., the personal appraisal of protecting one's privacy) as well as self-efficacy (i.e., confidence in one's privacy protection abilities) are reliable correlates of privacy behavior (Baruh et al., 2017; Chen & Chen, 2015; Dienlin & Metzger, 2016; Dienlin & Trepte, 2015; Youn, 2009). However, the theory of planned behavior posits that besides attitudes and self-efficacy, subjective norms also influence behavioral intentions. Drawing on prior work, we argue that subjective norms are also connected to privacy attitudes and self-efficacy, suggesting that the latter are shaped by societal, culture-specific norms: Dogruel and Jöckel (2019) revealed that norms manifested in the national privacy governance system in the United States versus Germany influence how much people feel in control over their data, which can be conceptualized as an aspect of self-efficacy. Research has proposed that self-efficacy is influenced, inter alia, by physiological factors (e.g., stressful situations) and personal experience; it is also affected by vicarious experience (e.g., "if they can do it, I can do it too") and social persuasion (Bandura, 1977), which indicates that privacy protective behavior exemplified by peers could set behavioral norms shaping social media users' privacy self-efficacy.

Following this logic on the influence of normative information, Trepte et al. (2015) proposed a social desirability hypothesis, arguing that norms and group pressure about how desirable it is to protect personal data online could foster people's attitudes toward online privacy and perceived risks. As posited by the bandwagon effect (Nadeau et al., 1993), peer norms have an impact on people's attitudes which, in turn, could explain why normative information in the form of explicit social cues (e.g., "67% of other users limited the visibility of their profile") can enhance users' privacy-protection behavior (Spottswood & Hancock, 2017). Prior research has demonstrated that privacy policy compliance can be influenced by informal social learning and vicarious experience (Warkentin et al., 2011). Therefore, we suggest that perceived privacy norms will influence both social media users' attitudes, including risk perceptions, and self-efficacy toward their online privacy:

Hypothesis 5 (H5). Subjective privacy norms toward privacy protection are positively associated with (a) perceived privacy risks, (b) attitudes toward online privacy, and (c) privacy self-efficacy.

Subjective privacy norms are likely also culturally specific since the social environment, here represented by the national privacy regulatory approach as discussed earlier, is believed to cultivate privacy rules that are reflected in users' own subjective privacy norms. Thus, we combine the suggestion that (a) subjective privacy norms may explain cross-national differences regarding privacy protection and self-disclosure and (b) perceptions of norms may be associated with privacy attitudes, risks, and self-efficacy. Our final research question asks:

Research Question 1 (RQ1). To what extent can cross-national differences in online privacy protection and self-disclosure be explained by a serial mediation of subjective privacy norms followed by privacy attitudes, risks, and privacy self-efficacy?

Method

This study's materials, including the questionnaire, data, syntax, and supplementary analyses, can be accessed at https://osf.io/7kazy/.

Sample

Data were collected in the United States and Germany surveying adult Facebook users. The sample consisted of 1,060 participants, including 539 US participants (301 female, 238 male) with a mean age of $M=36.73$ ($SD=11.20$; range: 18–75) and 521 German participants (250 female, 271 male) with a mean age of $M=36.66$ ($SD=13.62$; range: 14–81). Participants in the US sample were recruited in December 2017 from MTurk, with the requirement that they are residents of the United States. The German sample was recruited in October 2017 using an online access panel. The frequency of Facebook use (measured on a 6-point scale from 1=*not at all* to 6=*several times a day*) did not vary significantly between participants from both countries (United States: $M=5.38$, $SD=1.00$; Germany: $M=5.26$, $SD=1.15$; $t(1,029.18)=1.88$, $p=.061$, *Cohen's d*=0.12). More information about cross-national differences in social media use is displayed in Table A1.

Measures

To ensure that cross-national differences are not due to translation inaccuracies, the first author translated every item of the measures and a student assistant backtranslated it to the original language. If divergences between languages were found, modifications were made. The modifications were confirmed by native speakers of English and German. We ran a confirmatory factor analysis (CFA) for each variable. Fit indices, psychometric information, Cronbach's alpha, composite reliability omega, and average variance extracted (AVE) are displayed in the supplementary material (https://osf.io/z7fp8 and https://osf.io/7kazy).

Subjective privacy norms were measured on a 5-point scale with nine original items on three different levels: norms (a) among peers, (b) in society in general, and (c) in news media coverage.

To provide a more nuanced view of *privacy risks*, recent research has differentiated between expected violations of privacy on a horizontal (i.e., peers may violate one's privacy) and vertical (i.e., companies or the government may violate one's privacy) level (Masur, 2018). Six original items were used to measure participants' horizontal and vertical perceived privacy risks online on a 5-point scale.

Participants' *online privacy attitudes* were measured using Dienlin and Trepte's (2015) 7-point sematic differential scale, subdivided into informational, psychological, and social privacy attitudes. When necessary, participants' answers were recoded so that higher means reflected more favorable attitudes toward online privacy protection.

With eight items adapted from Dienlin and Metzger (2016), Krasnova et al. (2010), as well as Youn (2009), we measured on a 5-point scale participants' online *privacy self-efficacy* on a vertical and horizontal level.

To assess participants' *privacy protection behavior*, they indicated whether they ever took one or more of 10 possible actions on Facebook to protect their privacy with answer options 0=*no* or 1=*yes* (e.g., withdrawing information about the self or untagging pictures). Statistics for these items in each country is included in Table A2. Only six out of these items were unidimensional (see Table A3; see asterisks in the questionnaire).

Self-disclosure of personal information disclosure, emotions, and political opinions were measured. Participants' personal information disclosure was measured on a 5-point scale using five items (which indicated unidimensionality; see Table A3; see asterisks in the questionnaire) from Metzger and Suh (2017). Disclosure of emotions on Facebook was measured on a 5-point scale adapted from Miller et al. (1983) subdivided into public and private disclosure. Participants' disclosure of political opinions was measured with eight original items on a 5-point scale, subdivided into public and private channels.

Data Analysis

Hypotheses and *RQ1* were tested using software SPSS (version 25.0) and *R* (Version 3.5.3) with its package lavaan (Rosseel, 2012). *H1–H3* were addressed based on a *t*-test for independent sample, while *H4, H5*, and *RQ1* were examined by structural equation modeling (SEM) with maximum likelihood estimation.

Results

H1 predicted that Germans disclose less information about themselves on SNS than US users. As shown in Table 1, this hypothesis was supported with small effects (*Cohen's d*: 0.17 – 0.33): German Facebook users indicated that they disclose less personal information, emotions, and political opinions than US Facebook users. A more nuanced analysis of the different channels people use to express themselves (see Table A4) indicates that when it comes to disclosing emotional states, German and US Facebook users divulge a similarly low level of emotions on public Facebook channels ($d=-0.02$). In private Facebook channels (e.g., messenger), US users disclose emotions to a greater extent than German users ($d=0.30$). The pattern is clearer regarding political opinions: In both private ($d=0.33$) and public ($d=0.27$) Facebook channels, US users are more likely to express political opinions than are German users.

H2 expected that German SNS users would take more measures to protect their privacy than US SNS users. Results, though, revealed that the opposite is the case: Out of six potential measures to be taken, US Facebook users make use of $M=2.65$ ($SD=1.47$), while German Facebook users take $M=2.23$ ($SD=1.48$) measures (see Table 1). US Facebook users protect themselves more than German users on all items except using a pseudonym. Results do not corroborate *H2* but revealed a small and opposite cross-national effect ($d=0.29$).

With *H3*, it was hypothesized that German SNS users would perceive stronger subjective norms to protect their online privacy than US SNS users. Table 1 indicates that the

Table 1. Cross-National Differences of Self-Disclosure, Privacy Protection, Privacy Norms, Risks, Attitudes, and Self-Efficacy.

Variable	USA		Germany		*t*	*df*	*p*	*LL*	*UL*	*Cohen's d*
	M	*SD*	*M*	*SD*						
Disclosure: Personal information	2.80	0.94	2.52	0.90	4.88	1,058	<.001	.17	.39	0.30
Disclosure: Emotions	2.17	0.84	2.02	0.88	2.77	1,058	.006	.04	.25	0.17
Disclosure: Political opinions	2.42	1.20	2.05	1.06	5.30	1,050.59	<.001	.23	.50	0.33
Privacy protection behavior	2.65	1.47	2.23	1.48	4.67	1,058	<.001	.25	.60	0.29
Subjective privacy norms	3.55	0.74	3.38	0.69	3.82	1,058	<.001	.08	.25	0.24
Privacy risks	3.27	0.99	3.25	0.95	0.31	1,058	.756	−.10	.13	0.02
Privacy attitudes	4.61	0.79	4.69	0.80	−1.54	1,058	.124	−.17	.02	−0.10
Privacy self-efficacy	2.83	0.99	2.81	0.87	0.37	1,049.09	.714	−.09	.13	0.02

LL and UL refer to the lower and upper limit of the 95% confidence interval of the difference.

opposite applies: US participants stated stronger subjective privacy norms than German participants ($d=0.24$). When analyzing subjective norms on different levels, Table A4 demonstrates that the differences predominantly apply for perceived norms at the peers ($d=0.29$) and national ($d=0.39$) levels, but not subjective norms conveyed via the media. Thus, the data do not support *H3* but rather indicate a small opposite effect.

H4, *H5*, and *RQ1* were examined by structural equation modeling, with nation (United States vs Germany) as an independent variable, subjective norms, privacy attitudes, risks, and self-efficacy in a serial mediation, and privacy protection behavior and self-disclosure as dependent variables (see Figure 1). Zero-order correlations among all variables are displayed in Table 2. Since the dimension "social privacy attitudes" indicated a negative low loading for the latent variable "privacy attitudes," the variable was removed from the model. The model fit was acceptable, χ^2 (59)=388.27, $p<.001$, CFI=.91, TLI=.86, RMSEA=.08 (90% confidence interval from .069 to .084), SRMR=.06. *H4* expected subjective norms to mediate the cross-national effects on privacy protection and self-disclosure behavior. All indirect and total effects are shown in Table 3. First, it should be noted that subjective privacy norms were not associated with protective behavior, β=.04, $b=.19$, $SE_b=.18$, 95% CI = [−.16, .53], $z=1.05$, $p=.296$, but weakly related to self-disclosure, β=.13, $b=.24$, $SE_b=.07$, 95% CI = [.09, .38], $z=3.25$, $p=.001$. Thus, the model indicated no indirect effect through subjective norms on protection behavior, β=−.01, $p=.306$, but a very small, albeit significant, indirect effect on self-disclosure, β=−.02, $p=.005$ (see Table 3). Although the data partly support *H4*, the size of the significant indirect effect is too small to be considered theoretically relevant.

Contrary to expectations in H5*a*, subjective norms were not positively related to perceived privacy risks, β=.08, $b=.12$, $SE_b=.07$, 95% CI = [−.01, .25], $z=1.76$, $p=.078$, but rather were negatively, albeit very weakly, associated with privacy attitudes, β=−.15, $b=-.25$, $SE_b=.09$, 95% CI = [−.42, −.08], $z=-2.90$, $p=.004$, revealing a relationship opposite to the expectations in *H5b*. Supporting *H5c*, the model indicated a positive and medium association between subjective norms and privacy self-efficacy, β=.34, $b=.64$, $SE_b=.09$, 95% CI = [.47, .80], $z=7.48$, $p<.001$.

The model also showed that perceived privacy risks were positively, albeit very weakly, associated with protection behavior, β=.12, $b=.35$, $SE_b=.14$, 95% CI = [.08, .62], $z=2.55$, $p=.011$, and self-disclosure, β=.21, $b=.26$, $SE_b=.06$, 95% CI = [.13, .39], $z=4.03$, $p<.001$. Online privacy attitudes had a small positive correlation with protection behavior, β=.23, $b=.60$, $SE_b=.15$, 95% CI = [.32, .88], $z=4.15$, $p<.001$, and a medium negative correlation with self-disclosure, β=−.60, $b=-.65$, $SE_b=.08$, 95% CI = [−.80, −.50], $z=-8.39$, $p<.001$. Privacy self-efficacy, however, was neither related to protection behavior, β=.01, $b=.02$, $SE_b=.10$, 95% CI = [−.19, .22], $z=0.17$, $p=.863$, nor to self-disclosure, β=.08, $b=.08$, $SE_b=.05$, 95% CI = [−.02, .18], $z=1.55$, $p=.122$.

Concerning *RQ1*, Table 3 reveals that cross-national effects on protective behavior and self-disclosure can only be explained through the serial mediation of subjective norms and privacy attitudes. The relationships in this model indicate that subjective norms can reduce favorable attitudes toward privacy protection while the latter increases privacy protection and lowers self-disclosure. Despite reaching statistical significance, these indirect effects through subjective norms and privacy attitudes were very small (protection behavior: β=.01, $p=.024$, self-disclosure: β=−.02, $p=.012$).

Discussion

By focusing on how subjective norms influence micro-level personal privacy management behavior and are themselves influenced by the macro-level national cultural context, this study sheds new light on the role that social norms play in shaping social media users' privacy attitudes and behavior.

Cross-National Differences in Privacy Behavior

Results for the first hypothesis are consistent with previous findings (e.g., Krasnova & Veltri, 2010) but give a

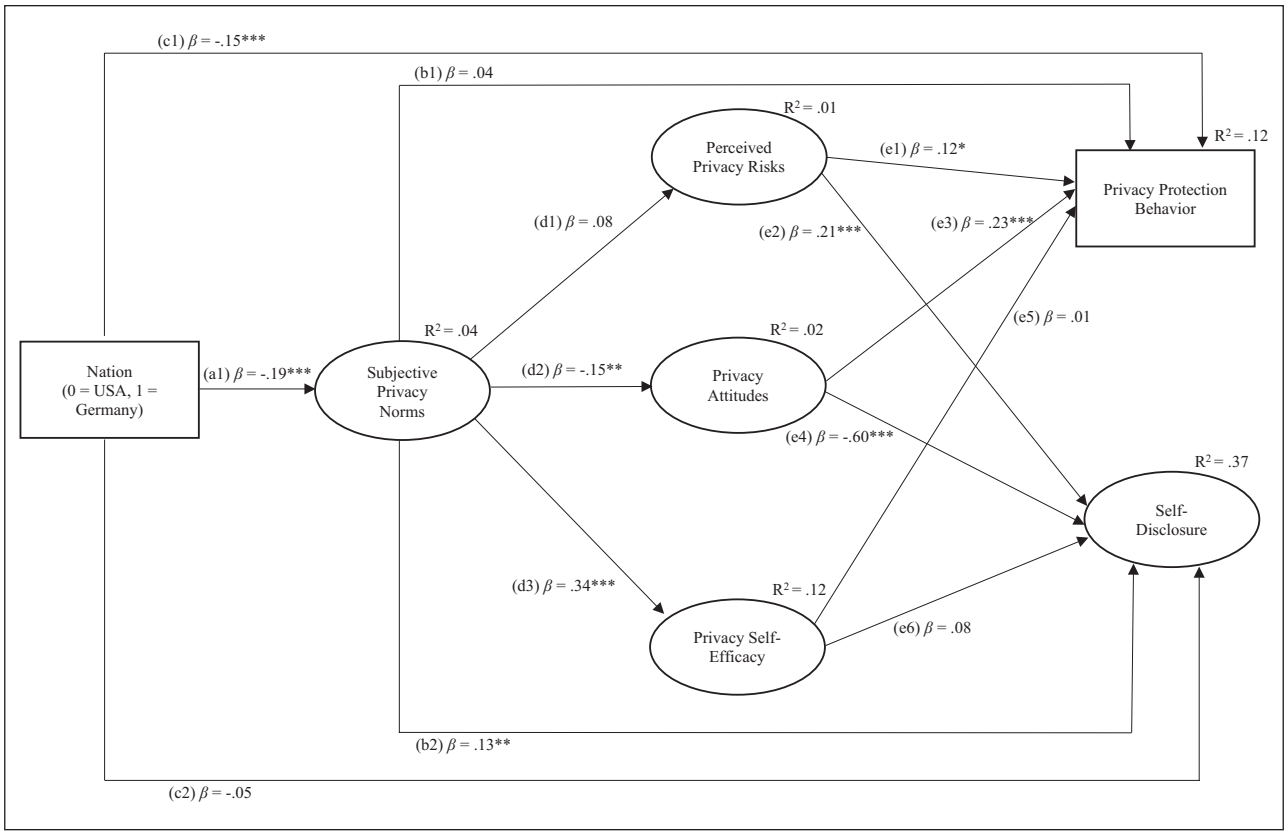

Figure 1. Structural equation model including standardized coefficients of direct effects.
***$p < .001$, **$p < .01$, *$p < .05$.

Table 2. Zero-Order Correlations.

	1.	2.	3.	4.	5.	6.	7.
1. Disclosure: Personal information	–						
2. Disclosure: Emotions	.506**	–					
3. Disclosure: Political opinions	.459**	.563**	–				
4. Privacy protection behavior	−.162**	−.027	−.029	–			
5. Subjective privacy norms	.220**	.089**	.069*	.051	–		
6. Privacy risks	−.080**	.071*	.027	.157**	.100**	–	
7. Privacy attitudes	−.427**	−.248**	−.228**	.279**	−.010	.325**	–
8. Privacy self-efficacy	.317**	.169**	.128**	−.129**	.267**	−.224**	−.349**

***$p < .001$, **$p < .01$, *$p < .05$.

more nuanced view of the *content* people disclose across nations. While US users disclose more personal information and political opinions than German users, when it comes to disclosing emotions in public channels, the cross-national differences are smaller. This might suggest there is an implicit "rule" or social norm that emotions should not be expressed in channels in which the audience is uncontrollable across all or some cultures. Such a social norm may be more universal than norms concerning political expression, which likely vary nationally according to the debate culture of a specific country. In any case, results provide some preliminary evidence that privacy behaviors differ at the national level, potentially through subjective norms.

The results of the second hypothesis provide further evidence that national culture affects privacy protection behavior, although not as expected in that Germans did not take more measures to protect themselves in social media than Americans. There are several potential explanations for this unanticipated result. One is that US users may feel greater motivation to protect themselves because they disclose more on social media compared with German users. Another explanation is that Germans may feel less need to implement privacy protections in SNSs because they feel better

Table 3. Indirect and Total Effects.

	β	*b*	SE_b	95% CI [lower/upper]	*z*	*p*
Indirect effects						
a1b1: Nation ⩾ norms ⩾ protection	−.01	−.03	.03	−.10/.03	−1.02	.306
a1b2: Nation ⩾ norms ⩾ self-disclosure	−.02	−.04	.02	−.08/−.01	−2.84	.005
a1d1e1: Nation ⩾ norms ⩾ risks ⩾ protection	−.00	−.01	.01	−.02/.00	−1.40	.161
a1d1e2: Nation ⩾ norms ⩾ risks ⩾ self-disclosure	−.00	−.01	.00	−.01/.00	−1.55	.121
a1d2e3: Nation ⩾ norms ⩾ attitudes ⩾ protection	.01	.03	.01	.00/.05	2.26	.024
a1d2e4: Nation ⩾ norms ⩾ attitudes ⩾ self-disclosure	−.02	−.03	.01	−.05/−.01	−2.52	.012
a1d3e5: Nation ⩾ norms ⩾ self-efficacy ⩾ protection	−.00	−.00	.01	−.03/.02	−.17	.863
a1d3e6: Nation ⩾ norms ⩾ self-efficacy ⩾ self-disclosure	−.01	−.01	.01	−.02/.00	−1.47	.141
Total effects						
Privacy protection behavior	−.15	−.64	.13	−.90/−.38	−4.84	<.001
Self-disclosure	−.08	−.14	.05	−.24/−.04	−2.74	.006

protected by their government's privacy policy (e.g., the GDPR). By contrast, Americans may feel more vulnerable by virtue of less government and legal protections, and so feel that it is their personal responsibility to protect their data, especially if they disclose to a greater extent. In other words, the subjective norms directing privacy behavior promoted by the sociopolitical environment in the United States might come from more of an individualistic "take care of your privacy yourself" approach, whereas the norms in Germany might stem from more of a collectivistic "our government takes care of our privacy" approach. This interpretation is further corroborated by exploratory analyses (see Table A5 in the supplementary material, https://osf.io/z7fp8 and https://osf.io/7kazy): Americans believe more strongly than Germans that privacy is a right that needs to be defended ($d=0.22$) and that should be part of the Constitution ($d=0.15$). At first glance, this result might appear surprising, still, these different views on privacy could be a result of different governmental approaches, leading Americans to perceive a stronger "need for action" in terms of protecting their privacy.

Cross-National Differences in Subjective Privacy Norms

The fact that subjective norms to protect one's privacy in SNSs are stronger in the United States compared with Germany corroborates the explanation that US users feel their sociopolitical environment places the protection responsibility on individual users. While this is opposite to what was expected, the same explanation as above may apply to why Germans perceived less strong subjective norms to protect their privacy: If Germans feel government privacy policy already protects them, there may be less discussion from both peers and at the national level about the imperative for individuals to protect their privacy. While this explanation requires further examination, our initial findings support our idea that national culture shapes privacy attitudes and behavior, but in a different, more macro-level way than we originally theorized. As shown in Table A4 (see supplementary material, https://osf.io/z7fp8 and https://osf.io/7kazy), the difference between US and German users was greater for subjective privacy norms on the national level than it was on the level of a peer group such as family/friends, which further supports the notion that privacy rules manifested in social norms vary most strikingly across national boundaries.

In sum, our findings underline that while privacy rules are important for personal privacy regulation (Petronio, 2002), these rules manifest themselves differently from what we hypothesized because it may be that subjective norms at both peer *and* national levels may be important predictors of privacy behavior at the personal level. This presents a new interpretation of how subjective norms may operate to influence individuals' privacy behavior, and we hope it will open a new line of investigation into how macro-level social forces affect micro-level privacy behavior.

The Relationship between Subjective Norms and Privacy Attitudes, Risks, and Self-Efficacy

We hypothesized that subjective norms to protect one's privacy would ameliorate users' attitudes to protect their privacy. On a bivariate analytical level, no relationship between those variables emerged. In a multivariate analysis (the SEM), stronger subjective privacy norms were associated with *less* positive attitudes to protect their privacy. This might be explained by psychological reactance in the sense that people are less willing to comply with a rule if they feel pressured to do so (Brehm & Brehm, 2013). Regardless, the bottom line is that, even if privacy rules expressed as subjective norms about self-protection are perceived as strong, it does not mean that they manifest themselves in more favorable attitudes toward protection. This is also reflected in the

fact that subjective privacy norms were positively, albeit weakly, associated with self-disclosure in the multivariate analysis (although not in the bivariate analysis).

Despite the unexpected negative association between subjective norms and privacy protection attitudes, our data show that more favorable attitudes toward privacy protection are associated with (slightly) greater actual protection behavior and less disclosure. This finding adds to recent research that provides evidence against the privacy paradox (see Baruh et al., 2017 for a review). Also interesting is that while perceived privacy risks correlated weakly but positively with protection behavior (replicating findings by Dienlin & Metzger, 2016), they also correlated positively with self-disclosure (contradicting findings by Dienlin & Metzger, 2016). An explanation for this set of relationships could be that risk triggers a serial process that ultimately reduces barriers to disclosure, similar to the process proposed by Chen and Chen (2015) described earlier: Greater risk motivates more self-protection (e.g., limiting the audience for one's posts), which then prompts greater disclosure.

Our findings can also speak of the *nature* of the self-disclosure. Disclosure of different types of information might affect users' privacy attitudes and protection behaviors in different ways. Unlike most prior research, in our study self-disclosure included relatively and interpersonally risky actions such as expressing one's political opinions and emotions. Thus, it is conceivable that participants who are primed to think about this type of disclosure are more likely to consider risks (e.g., harmful comments resulting from expressing political opinions), and thus trigger the serial process mentioned above. Alternatively, the act of disclosing risky information and experiencing negative consequences may itself heighten risk perceptions, indicating that the association between self-disclosure and perception of risks could be reciprocal. In any case, this indicates a need for future privacy research to not measure self-disclosure generally but rather disclosure of specific types of content, as the nature of the disclosure can elicit greater or lesser privacy risks, which in turn affects privacy protection behavior and self-disclosure.

Our data also show that subjective norms about privacy positively relate to self-efficacy to protect oneself. The more people glean from their social environment that protecting one's privacy on SNS is desirable, the more confident they seem to feel about their ability to do so. An implication of this finding is that for users with lower levels of privacy self-efficacy, promoting privacy norms in society may help to empower them. However, it is still a question whether greater privacy self-efficacy results in more protection behavior. On a bivariate level, our results show that privacy self-efficacy is negatively, albeit weakly, associated with protective privacy behavior and also positively with self-disclosure. In the SEM, no effects were detectable (corroborating findings by Dienlin & Metzger, 2016). It is also interesting that subjective norms increase self-efficacy yet, as described earlier, decrease privacy protection attitudes. According to the theory of planned behavior, both should be present to foster corresponding behavior. It may be the case that if attitudes toward privacy protection are not positive, self-efficacy will be meaningless. This could explain the weak and/or nonsignificant effects on privacy protection behavior and self-disclosure. At the very least, we can say that the relationship between privacy self-efficacy and protecting and expressing oneself in social media requires further studies to be fully understood, and that our findings suggest that one potential source for higher privacy self-efficacy could be strengthening the subjective norm at the national level.

Theoretical Implications

Looking across our study as a whole, results are in line with Petronio's (2002) proposition that people use a rule-based management system to regulate their privacy by showing that subjective norms help to explain people's personal privacy regulation and, as expected, there seem to be some cross-national differences toward these norms. That said, the role of subjective norms as traditionally conceptualized at the individual level was not as strong as we expected. Instead, the results uncovered macro-level normative mechanisms suggesting that differences in governmental regulation shape subjective norms about privacy in a way that it either shoulders protection responsibility to the individual (in the United States) or to the government (in Germany/EU). In any case, this study shows that the psychological processes driving personal privacy regulation are more complex than originally thought and subject to both micro- and macro-level sociopolitical forces.

Our study also extends cross-cultural privacy research by using a novel means to understand cultural differences in privacy attitudes and behavior. Previous cross-cultural privacy research has mostly focused on individualism-collectivism to differentiate cultures, which has been heavily criticized in the face of globalization and has produced confusing results. By contrast, we explore how cross-national differences in governmental privacy regulation may be reflected in citizens' perceptions of social norms.

Limitations

That said, as a limitation of this work, subjective norms are only one type of social norms, future research could also look into "injunctive" (norms based on threat of disapproval from others) and "descriptive" (norms based on observations of what others do) behavioral norms to explain more variance in privacy attitudes and behavior. Moreover, while this study considered privacy behavior through a cultural lens offering perceived subjective norms as a connecting variable, we acknowledge that norms at any level are only one piece of the puzzle and that situational,

motivational, regional, gender, and other factors also need to be considered (Petronio, 2002). For example, situational and motivational factors (e.g., the desire to receive social gratifications) or abilities (e.g., having the cognitive resources to practice protective behavior) surely also play an important role in explaining whether, when, and how individuals decide to protect their privacy on social media. Another limitation of this work lies in the fact that our connection between different regulatory systems and subjective norms is tested only implicitly. While an explicit test appears difficult to conduct, further research replicating cross-national effects could corroborate the role different governmental approaches shape privacy rules in the form of social norms. Especially the fact that different governmental contexts have different political structures and have different systems to pass (privacy) laws needs to be considered. With that said, subjective privacy norms could also be connected to people's political leaning and environment to test whether the processes outlined here vary across party lines. Finally, direct measures of citizens' privacy regulation literacy (e.g., knowledge of existing privacy regulation and/or the degree to which people feel the government protects their privacy) or whether they view privacy as a human right would also be informative and should be included in future research.

Conclusion

This work extends (online) privacy research by pointing to a hitherto understudied explanation for why people's privacy regulation behavior varies across national boundaries. Drawing on Petronio's (2002) rule-based privacy management system, we argued that the national context and the associated particular governmental approach to deal with privacy protection shapes people's subjective norms about privacy. Overall, we provide evidence that not only privacy behaviors, but also subjective privacy norms differ at the national level. This evidence could not only provoke further research to take the macro-level of analysis (e.g., national context) into account more systematically, but also to consider the explanatory value of "privacy rules" in the form of subjective norms in a serial process that unravels the complexity of human beings' privacy behavior in both online and offline communication channels.

Declaration of Conflicting Interests

The author(s) declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

Funding

The author(s) disclosed receipt of the following financial support for the research, authorship, and/or publication of this article: This research was funded by the German Federal Ministry of Education and Research (BMBF, Funding number: 16KIS0743).

ORCID iDs

German Neubaum https://orcid.org/0000-0002-7006-7089
Miriam Metzger https://orcid.org/0000-0001-8433-8604
Nicole Krämer https://orcid.org/0000-0001-7535-870X

Supplemental Material

Supplemental material for this article is available online.

References

Acquisti, A., Brandimarte, L., & Loewenstein, G. (2015). Privacy and human behavior in the age of information. *Science*, *347*(6221), 509–514. https://doi.org/10.1126/science.aaa1465

Altman, I. (1975). *The environment and social behavior: Privacy, personal space, territory, crowding*. Brooks/Cole.

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

Bandura, A. (1977). Self-efficacy: Toward a unifying theory of behavioral change. *Psychological Review*, *84*(2), 191–215. https://doi.org/10.1037/0033-295X.84.2.191

Baruh, L., Secinti, E., & Cemalcilar, Z. (2017). Online privacy concerns and privacy management: A meta-analytical review. *Journal of Communication*, *67*(1), 26–53. https://doi.org/10.1111/jcom.12276

Bellman, S., Johnson, E. J., Kobrin, S. J., & Lohse, G. L. (2004). International differences in information privacy concerns: A global survey of consumers. *The Information Society*, *20*(5), 313–324. https://doi.org/10.1080/01972240490507956

Blanchette, J.-F., & Johnson, D. G. (2002). Data retention and the panoptic society: The social benefits of forgetfulness. *The Information Society*, *18*(1), 33–45. https://doi.org/10.1080/01972240252818216

Boyne, S. M. (2018). Data protection in the United States. *The American Journal of Comparative Law*, *66*(Suppl. 1), 299–343. https://doi.org/10.1093/ajcl/avy016

Brehm, S. S., & Brehm, J. W. (2013). *Psychological reactance: A theory of freedom and control*. Academic Press.

Budak, J., Rajh, E., & Recher, V. (2017). Citizens' privacy concerns: Does national culture matter? In M. Friedewald, J. P. Burgess, J. Čas, R. Bellanova, & W. Peissl (Eds.), *Surveillance, privacy and security—Citizens' perspectives* (pp. 36–51). Springer.

Chen, H.-T. (2018). Revisiting the privacy paradox on social media with an extended privacy calculus model. *American Behavioral Scientist*, *62*(10), 1392–1412. https://doi.org/10.1177/0002764218792691

Chen, H.-T., & Chen, W. (2015). Couldn't or wouldn't? The influence of privacy concerns and self-efficacy in privacy management on privacy protection. *Cyberpsychology, Behavior, and Social Networking*, *18*(1), 13–19. https://doi.org/10.1089/cyber.2014.0456

Child, J. T., & Petronio, S. (2011). Unpacking the paradoxes of privacy in CMC relationships: The challenges of blogging and relational communication on the Internet. In K. Wright & L. Webb (Eds.), *Computer mediated communication in personal relationships* (pp. 21–40). Hampton Press.

Cho, H., Knijnenburg, B., Kobsa, A., & Li, Y. (2018). Collective privacy management in social media: A cross-cultural validation. *ACM Transactions on Computer-human Interaction*, *25*(3), 1–33. https://doi.org/10.1145/3193120

Cho, H., Rivera-Sánchez, M., & Lim, S. S. (2009). A multinational study on online privacy: Global concerns and local responses. *New Media & Society*, *11*(3), 395–416. https://doi.org/10.1177/1461444808101618

Cialdini, R. B., & Trost, M. R. (1998). Social influence: Social norms, conformity and compliance. In S. T. Fiske & G. Lindzey (Eds.), *The handbook of social psychology* (Vol. 2, pp. 151–192). McGraw-Hill.

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*, *21*(5), 368–383. https://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: The relation between privacy attitudes and privacy behaviors. *European Journal of Social Psychology*, *45*(3), 285–297. https://doi.org/10.1002/ejsp.2049

Dogruel, L., & Jöckel, S. (2019). Risk perception and privacy regulation preferences from a cross-cultural perspective. A qualitative study among German and US smartphone users. *International Journal of Communication*, *13*, 9824.

Hallinan, D., Friedewald, M., & McCarthy, P. (2012). Citizens' perceptions of data protection and privacy in Europe. *Computer Law & Security Review*, *28*(3), 263–272. https://doi.org/10.1016/j.clsr.2012.03.005

Hofstede, G. H. (1997). *Cultures and organizations: Software of the mind* (Rev. ed.). McGraw-Hill.

Kokolakis, S. (2017). Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. *Computers & Security*, 64, 122–134. https://doi.org/10.1016/j.cose.2015.07.002

Krasnova, H., Spiekermann, S., Koroleva, K., & Hildebrand, T. (2010). Online social networks: Why we disclose. *Journal of Information Technology*, *25*(2), 109–125. https://doi.org/10.1057/jit.2010.6

Krasnova, H., & Veltri, N. F. (2010). Privacy calculus on social networking sites: Explorative evidence from Germany and USA. In *2010 43rd Hawaii international conference on system sciences* (pp. 1–10). https://www.academia.edu/12022497/Privacy_calculus_on_social_networking_sites_Explorative_evidence_from_Germany_and_USA

Lewis, K., Kaufman, J., & Christakis, N. (2008). The taste for privacy: An analysis of college student privacy settings in an online social network. *Journal of Computer-mediated Communication*, *14*(1), 79–100. https://doi.org/10.1111/j.1083-6101.2008.01432.x

Liang, H., Shen, F., & Fu, K. (2017). Privacy protection and self-disclosure across societies: A study of global Twitter users. *New Media & Society*, *19*(9), 1476–1497. https://doi.org/10.1177/1461444816642210

Liu, Z., & Wang, X. (2018). How to regulate individuals' privacy boundaries on social network sites: A cross-cultural comparison. *Information & Management*, *55*(8), 1005–1023. https://doi.org/10.1016/j.im.2018.05.006

Masur, P. K. (2018). *Situational privacy and self-disclosure: Communication processes in online environments*. Springer.

Masur, P. K., DiFranzo, D., & Bazarova, N. N. (2021). Behavioral contagion on social media: Effects of social norms, design interventions, and critical media literacy on self-disclosure. *PLOS ONE*, *16*(7), e0254670. https://doi.org/10.1371/journal.pone.0254670

Metzger, M. J., & Suh, J. J. (2017). Comparative optimism about privacy risks on Facebook: Comparative optimism about privacy risks. *Journal of Communication*, *67*(2), 203–232. https://doi.org/10.1111/jcom.12290

Miller, L. C., Berg, J. H., & Archer, R. L. (1983). Openers: Individuals who elicit intimate self-disclosure. *Journal of Personality and Social Psychology*, *44*(6), 1234.

Movius, L. B., & Krup, N. (2009). U.S. and EU privacy policy: Comparison of regulatory approaches. *International Journal of Communication*, *3*, 169–187.

Nadeau, R., Cloutier, E., & Guay, J.-H. (1993). New evidence about the existence of a Bandwagon effect in the opinion formation process. *International Political Science Review*, *14*(2), 203–213. https://doi.org/10.1177/019251219301400204

Napoli, P. M., & Dwyer, D. L. (2018). U.S. media policy in a time of political polarization and technological evolution. *Publizistik*, 63, 583–601. https://doi.org/10.1007/s11616-018-0440-2

Petronio, S., & Child, J. T. (2020). Conceptualization and operationalization: Utility of communication privacy management theory. *Current Opinion in Psychology*, 31, 76–82. https://doi.org/10.1016/j.copsyc.2019.08.009

Petronio, S. S. (2002). *Boundaries of privacy: Dialectics of disclosure*. State University of New York Press.

Pleger, L. E., Guirguis, K., & Mertes, A. (2021). Making public concerns tangible: An empirical study of German and UK citizens' perception of data protection and data security. *Computers in Human Behavior*, *122*, 106830. https://doi.org/10.1016/j.chb.2021.106830

Rosseel, Y. (2012). Lavaan: An R Package for structural equation modeling. *Journal of Statistical Software*, *48*(2), 1–36. https://doi.org/10.18637/jss.v048.i02

Rui, J., & Stefanone, M. A. (2013). Strategic self-presentation online: A cross-cultural study. *Computers in Human Behavior*, *29*(1), 110–118. https://doi.org/10.1016/j.chb.2012.07.022

Shulman, H. C., Rhodes, N., Davidson, E., Ralston, R., Borghetti, L., & Morr, L. (2017). The state of the field of social norms research. *International Journal of Communication*, *11*, 22.

Spottswood, E. L., & Hancock, J. T. (2017). Should I share that? Prompting social norms that influence privacy behaviors on a social networking site. *Journal of Computer-mediated Communication*, *22*(2), 55–70. https://doi.org/10.1111/jcc4.12182

Trepte, S. (2020). The social media privacy model: Privacy and communication in the light of social media affordances. *Communication Theory*, *31*, 35. https://doi.org/10.1093/ct/qtz035

Trepte, S., & Masur, P. K. (2016). *Cultural differences in social media use, privacy, and self-disclosure: Research report on a multicultural study*. VU Amsterdam.

Trepte, S., Reinecke, L., Ellison, N. B., Quiring, O., Yao, M. Z., & Ziegele, M. (2017). A cross-cultural perspective on the privacy calculus. *Social Media + Society*, *3*(1), 205630511668803. https://doi.org/10.1177/2056305116688035

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. Law, Governance and Technology Series 20* (pp. 333–366). Springer.

Ur, B., & Wang, Y. (2013). A cross-cultural framework for protecting user privacy in online social media. *Proceedings of the 22nd international conference on World Wide Web—WWW '13*

Companion (pp. 755–762). https://www.blaseur.com/papers/ur_wang_psosm13_culturalframeworkslides.pdf

Utz, S., & Krämer, N. C. (2009). The privacy paradox on social network sites revisited: The role of individual characteristics and group norms. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace*, *3*(2), 2.

Vitak, J., Liao, Y., Mols, A., Trottier, D., Zimmer, M., Kumar, P. C., & Pridmore, J. (2022). When do data collection and use become a matter of concern? A cross-cultural comparison of US and Dutch privacy attitudes. *International Journal of Communication*, *17*, 28.

Vogels, E. A. (2021). 56% of Americans support more regulation of major technology companies. *Pew Research Center*. https://www.pewresearch.org/short-reads/2021/07/20/56-of-americans-support-more-regulation-of-major-technology-companies/#:~:text=Some%2056%25%20of%20Americans%20think,and%20influence%20in%20the%20economy

von Pape, T., Trepte, S., & Mothes, C. (2017). Privacy by disaster? Press coverage of privacy and digital technology. *European Journal of Communication*, *32*(3), 189–207. https://doi.org/10.1177/0267323117689994

Wang, X., & Liu, Z. (2019). Online engagement in social media: A cross-cultural comparison. *Computers in Human Behavior*, *97*, 137–150. https://doi.org/10.1016/j.chb.2019.03.014

Warkentin, M., Johnston, A. C., & Shropshire, J. (2011). The influence of the informal social learning environment on information privacy policy compliance efficacy and intention. *European Journal of Information Systems*, *20*(3), 267–284. https://doi.org/10.1057/ejis.2010.72

Westin, A. F. (1967). *Privacy and freedom*. Bodley Head.

Yang, K. C. C., & Kang, Y. (2015). Exploring big data and privacy in strategic communication campaigns: A cross-cultural study of mobile social media users' daily experiences. *International Journal of Strategic Communication*, *9*(2), 87–101. https://doi.org/10.1080/1553118X.2015.1008635

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. https://doi.org/10.1111/j.1745-6606.2009.01146.x

Zhang, X., Toru, S., & Kennedy, M. (2007). A cross-cultural analysis of privacy notices of the Global 2000. *Journal of Information Privacy and Security*, *3*(2), 18–36. https://doi.org/10.1080/15536548.2007.10855814

Author Biographies

German Neubaum (PhD, University of Duisburg-Essen) is an Assistant Professor of Psychological Processes of Education in Social Media at the University of Duisburg-Essen, Germany. His research interests focus on the educational benefits users can gain from using social media. By combining media psychological methods and social media analytics, he also studies the formation and the psychological effects of opinion homogeneity in online networks.

Miriam Metzger (PhD, University of Southern California) is Professor of Communication at the University of California at Santa Barbara. Her research lies at the intersection of media, information technology, and trust, centering on how information and communication technologies alter our understandings of privacy and credibility. Her work has been widely published in the field of communication and related disciplines, and she has coedited two volumes investigating issues of digital literacy. She also serves as Education Director of the Center for Information, Technology & Society (CITS) at UCSB.

Nicole Krämer (PhD, University of Cologne) is Professor of Social Psychology, Media and Communication at the University of Duisburg-Essen, Germany. Her research focuses on social psychological aspects of human-machine interaction (especially social effects of robots and virtual agents) and computer-mediated-communication. She investigates processes of information selection, opinion building, and relationship maintenance of people communicating via Internet, especially via social networking sites. She heads numerous projects that received third-party funding. She served as Editor-in-Chief of the *Journal of Media Psychology* (2015–2017), and she is currently Associate Editor of the *Journal of Computer Mediated Communication*.

Elias Kyewski (PhD, University of Duisburg-Essen) is a Lecturer at the Hochschule Ruhr West (Germany). His research focuses on psychological effects on new media, especially regarding hostile media perceptions and privacy regulation.

DOI: 10.1177/20563051231182365
URN: urn:nbn:de:hbz:465-20230825-173044-6