Human Communication Research ISSN 0360-3989

ORIGINAL RESEARCH

Transformative or Not? How Privacy Violation Experiences Influence Online Privacy Concerns and Online Information Disclosure

Philipp K. Masur [1] **& Sabine Trepte** [2]

1 Department of Communication Science, Vrije Universiteit Amsterdam, 1081 HV Amsterdam, The Netherlands
2 School of Communication, Department of Media Psychology, University of Hohenheim, 70593 Stuttgart, Germany

Previous research has shown that people seldom experience privacy violations while using the Internet, such as unwanted and unknown sharing of personal information, credit card fraud, or identity theft. With this study, we ask whether individuals' online privacy concerns increase and online information disclosure decreases if they experience such a worst-case scenario. Using representative data from a five-wave panel study ($n = 745$), we found that people who generally experience more privacy violations also have stronger privacy concerns (between-person differences). However, people who experienced more privacy violations than usual in the last 6 months were only slightly more concerned afterward and did not change their disclosure behavior afterward (within-person effects). The need for privacy moderated these processes. We untangle under which circumstances such experiences may be transformative, and discuss practical and conceptual consequences of how experiences translate into concerns, but not necessarily behaviors.

Keywords: Privacy Violations, Online Privacy Concerns, Online Information Disclosure, Longitudinal Analysis, Bayesian Statistics

doi:10.1093/hcr/hqaa012

Over the course of their lives, individuals experience moments of confidentiality and intimacy, but also intrusions into their personal or psychological space. Through these experiences, they develop a sense of privacy and learn to evaluate which environments provide a high level of privacy and which do not (Wolfe & Laufer, 1974). When physical privacy is violated, such assessments often emerge naturally (Acquisti, Brandimarte, & Loewenstein, 2015). However, in online

Corresponding author: Philipp K. Masur; e-mail: p.k.masur@vu.nl

environments where informational or psychological instead of physical privacy is invaded, such assessments are more difficult. By using social media, e-commerce websites, search engines, or other online service platforms, individuals disclose information and thereby create digital footprints that expose their preferences, personality, beliefs, and intentions to online service providers, governments, and other users. Privacy is threatened because personal information is collected, sold, and exploited for their economic value. At the same time, governments and intelligence agencies collect these data to implement mass surveillance practices (Greenwald, 2014). Privacy risks also increase because information disclosed online is persistent, searchable, replicable, and editable (boyd, 2008). Due to the corresponding scalability of online information and the blurring of the public and private spheres (Papacharissi, 2010), individuals who engage in online disclosure have a much higher risk that their personal information will be used in unintended ways.

In the present study, we ask whether individuals who have experienced one or more privacy violations online have higher online privacy concerns and reduce their online information disclosure. Previous research investigating the relationship between privacy violation experiences and privacy concerns suggests a positive but small relationship (e.g., Awad & Krishnan, 2006; Bansal, Zahedi, & Gefen, 2007; Büchi, Just, & Latzer, 2016; Smith, Milberg, & Burke, 1996; Xu, Teo, Tan, & Agarwal, 2012). Most of these studies were based on cross-sectional survey studies. The question of whether experiences change people's privacy concerns, however, refers not to *between-person* differences (as studied in cross-sectional surveys), but *within-person* processes.

In this article, we aimed to extend existing privacy theory by incorporating privacy violation experiences as relevant antecedents of online privacy concerns and online information disclosure, while taking differences in the need for informational privacy into account. In doing so, we explicitly disentangled between- and within-person processes to distinguish individual changes from interpersonal differences (cf. Voelkle, Brose, Schmiedek, & Lindenberger, 2014). To empirically test such assumptions on the between- *and* within-person level, a repeated-measurement design is needed (Hamaker, Kuiper, & Grasman, 2015). We hence conducted a representative five-wave longitudinal panel study. In doing so, we used a Bayesian estimation approach, which allows hypotheses to be tested against regions of practical equivalence (ROPE) rather than simply against "the null" (Kruschke & Liddell, 2018).

How experiences shape cognitions, attitudes, and protective behaviors

Having an experience means witnessing a particular event that leaves a more or less lasting impression that can be retrieved at a later point in time. Experiences can be regarded as a knowledge resource through which individuals construct, understand, and interpret their world. Individuals evaluate novel events or even entirely new contexts by drawing upon prior experiences in similar events or contexts.

Consequently, an unpleasant or traumatic personal experience should provide a motivational basis for preventive or protective behavior (Janoff-Bulmann & Schwartzberg, 1991). Weinstein (1989) proposed two explanations for such effects (p. 47): First, after personal experiences of hazards, crises, or other potentially harmful events, people judge the occurrence of such events as more probable and view themselves as potential future victims. This, in turn, leads to an increased interest in prevention. Second, personal experiences also lead individuals to think about the associated risks more frequently and with more clarity—again increasing the likelihood of engaging in preventative and protective behaviors.

The extended parallel process model (EPPM: Witte, 1998; Popova, 2012) further contextualizes these processes and proposes that a perceived threat that might result from a prior negative experience can lead to different responses depending on the nature of the perceived threat and response efficacy (i.e., the belief that one can indeed protect oneself against the threat). If a threat is severe enough and individuals perceive a high response efficacy, they should be motivated to protect themselves and engage in danger control strategies. If the threat is severe but response efficacy is low (i.e., one has the impression that one cannot do anything about it), individuals engage in fear control strategies instead. These include defense mechanisms such as message avoidance or minimization (Witte, 1998).

These theories of choice have frequently been criticized for relying too heavily on people's ability to engage in a rational expectation-based calculus to arrive at a decision (Loewenstein, Weber, Hsee, & Welch, 2001; Popova, 2012). More recent approaches note that emotional (instead of rational) reactions to risk or fear often drive behavior in unexpected and less cognitive ways (Loewenstein et al., 2001). This is partly mirrored in studies showing that negative online experiences such as aggressive online interactions influence people's emotional appraisal of online risks, but do not necessarily result in concrete actions to prevent them (Trepte, Dienlin, & Reinecke, 2014).

Privacy violation experiences in online environments

Much research in recent years has tried to conceptualize online privacy and studied how individuals perceive and handle privacy in online environments (for overviews, see e.g., Bélanger & Crossler, 2011; Masur, 2018; Trepte & Reinecke, 2011; van der Sloot & de Groot, 2018). Online privacy can be defined as an online user's individual assessment of how accessible they are while interacting with other users and institutions, and, whether they themselves can actively shape this level of accessibility through self-disclosure or privacy regulation (Trepte, 2020). Accordingly, we define privacy violations as unwanted access during an online interaction between an individual Internet user and other users or institutions. Whether and what an individual user perceives as a privacy violation crucially depends on the situation and the context (Masur, 2018; Nissenbaum, 2010; Solove, 2004). Online environments differ vastly with regard to how individuals interpret privacy (Choi & Bazarova,

2014). On social media, for example, sharing personal information in interpersonally connected networks is a fundamental aspect of the user experience (Bayer, Triệu, & Ellison, 2020). Consequently, experiences with personal data are "consistently imbricated with others" (Marwick & boyd, 2014, p. 2). This networked nature of online environments complicates privacy boundary management processes because the unwanted sharing of information may be caused by turbulences such as the intentional violation of previously established rules (e.g., sharing information with people outside the boundary), incorrect interpretations of rules (e.g., erroneous assumptions about who is permitted to possess the information), the emergence of fuzzy boundaries (e.g., through the imprecise communication of rules), dissimilar rule orientations (due to different socialization processes), and privacy dilemmas (e.g., accidentally becoming a member of a privacy boundary) (see communication privacy management theory; Petronio, 2002). Previous research has shown that privacy violations are particularly related to boundary turbulences such as stalking or harassment by others, spreading damaging rumors, and the unwanted sharing of personal information (e.g., Chen & Atkin, 2020; Debatin, Lovejoy, Horn, & Hughes, 2009; Trepte, Dienlin, & Reinecke, 2014).

In e-commerce settings, by contrast, buying and selling is the core purpose. This leads to a different kind of communication oriented toward the transaction of goods and services, and, most importantly, requires individuals to identify themselves and provide personal information such as their address or credit card information (Dinev & Hart, 2006). A fundamental privacy risk in this context relates to the constant accumulation of personal information and metadata and corresponding surveillance practices by commercial actors and institutions (Baruh & Popescu, 2017). However, such privacy invasions are largely invisible and leave individuals uncertain about whether and to what degree they should be concerned (Acquisti et al., 2015). Previous research has thus shown that the most prevalent perceived privacy violations refer to tangible information misuse such as financial fraud or identity theft (e.g., Chen & Atkin, 2020; Debatin et al., 2009).

In line with the general risk literature discussed earlier, the theory of situational privacy and self-disclosure (Masur, 2018) proposes that individuals post-situationally evaluate whether an online environment was appropriate for disclosing personal information and whether initial privacy regulation was successful. Here, online information disclosure refers to how much personal information a person shares on the Internet. Privacy regulation behaviors encompass all measures that individuals can take to manage their online privacy (ranging from choosing privacy-friendly over privacy-invasive platforms and applications to adapting platform-specific privacy settings or using pseudonyms; cf. Masur, 2018). If privacy violations occur (e.g., a recipient who was deemed trustworthy nonetheless shared information with an unwanted audience, information spreads unexpectedly in an environment that was initially deemed appropriate, or personal information was misused for financial fraud), these negative privacy violation experiences will both influence future privacy regulation behaviors (e.g., choosing other environments

that are deemed more appropriate) and inform situational assessments in similar contexts (e.g., deciding not to disclose or to disclose less information in similar environments). We therefore argue that individuals who have experienced a privacy violation judge the occurrence of such tangible invasions or turbulences as more probable and view themselves as potential future victims. This should correlate positively with concerns about online privacy as well as the likelihood of engaging in preventive behaviors (both privacy protection, such as using more strict privacy settings, *and* minimizing online information disclosure).

Differences between individuals or behavioral changes within individuals?

It is important to note that the outlined processes refer to *within-person* effects: An experience may *change* one's subsequent perceptions, attitudes, and behavior. Studies analyzing the relationship between privacy experiences and privacy concerns have often adopted such a within-person perspective to develop their hypotheses, but investigated between-person relationships with cross-sectional surveys instead. Scholars have long noted this discrepancy between theoretical reasoning and empirical investigations. Voelkle et al. (2014) noted that "[t]he vast majority of empirical research in the behavioral sciences is based on the analysis of between-person variation. In contrast, (. . .) the mechanisms specified by psychological theories generally operate within, rather than across, individuals" (p. 193). Therefore, following recent panel studies that aimed to disentangle between- and within-person effects (e.g., Dienlin, Masur, & Trepte, 2019; Keijsers et al., 2016), we explicitly discuss between- and within-person effects of privacy violation experiences on privacy concerns and information disclosure.

Between-person differences

In a first step, we can ask whether people who have experienced many privacy violations differ in their concerns and behaviors from people who have experienced few privacy violations. Prior research provides some initial support for a positive *between-person* relationship between privacy violation experiences and online privacy concerns. For example, Awad and Krishnan (2006) found that 532 respondents who believed that their privacy had been previously invaded also had stronger privacy concerns ($r = .12$). Likewise, Bansal et al. (2007) found that more privacy invasion experiences were correlated with higher concerns ($\beta = .20$) using the same single-item measure in the context of health-related information sharing in a survey of 367 students. Xu et al. (2012) conducted a survey of 198 participants and found that privacy violation experiences predicted privacy concerns ($\beta = .16$). Likewise, Büchi et al. (2016) found a small positive relationship between experienced privacy breaches on Facebook and online privacy attitudes ($\beta = .21$). These findings suggest a small- to medium-sized, positive between-person relationship between privacy violation experiences and privacy concerns.

H1a: Individuals who generally experience more privacy violations also have stronger online privacy concerns compared to people who generally experience fewer privacy violations (*between-person* relationship).

To our knowledge, however, no study has explicitly investigated whether privacy violation experiences and online information disclosure are correlated on the between-person level. That said, several studies have investigated the relationship between privacy violation experiences and privacy protection behavior. For example, based on a sample of 119 undergraduate students, Debatin et al. (2009) found that those who reported having experienced privacy invasions (such as unwanted advances, stalking, or harassment, damaging gossip or rumors, or theft or abuse of personal data) also indicated having changed their Facebook privacy settings. Based on 1,121 Swiss participants, Büchi et al. (2016) similarly found that people who indicated that their privacy had been violated online also reported having implemented more privacy protections, such as changing their SNS settings, using fake names, or deleting cookies ($\beta = .41$). However, this does not necessarily imply that privacy violation experiences are negatively *related* to information disclosure (assuming that disclosing less information is a way of protecting privacy). First, active privacy protection and information disclosure are not necessarily correlated, as they are influenced by different antecedents (e.g., Chen & Chen, 2015; Masur, 2018). Second, assuming that disclosing less is similar to actively protecting privacy again adopts a within-person perspective: It is reasonable to assume that prior experiences negatively affect information disclosure in the long run. On the between-person level, however, it is more likely that experiencing privacy violations should be positively related to online information disclosure, because more information disclosure increases the risk of becoming a victim of privacy violations. We hence hypothesize:

H1b: People who disclose personal information more frequently also experience more privacy violations (*between-person* relationship).

To identify and evaluate these between-person relationships with more precision, it is important to control for potential differences in people's need for informational privacy, which can be defined as "an individual's need to selectively control the access of others to the individual self with the aim of achieving a desired level of physical or psychological privacy" (Trepte & Masur, 2017). Child and Petronio (2011) similarly argue that "higher control needs are manifested in regulating privacy boundaries by controlling the flow of information to others" (p. 30). Awad and Krishnan (2006) found that the importance people ascribe to information transparency (a concept similar to the need for informational privacy) was indeed positively related to online privacy concerns ($r = .27$) and negatively related to a user's willingness to be profiled for personalized services ($r = -.12$) or personalized advertising ($r = -.17$). Based on 431 undergraduates, Yao, Rice, and Wallis (2007) found that the need for privacy is positively related to online privacy concerns ($\beta = .13$).

Similarly, Yao and Linz (2008) found that the need for privacy is positively related to privacy attitudes ($\beta = .18$). We thus hypothesize:

H2a: People with a stronger need for informational privacy also have stronger online privacy concerns (*between-person* correlation).
H2b: People with a stronger need for informational privacy disclose personal information online less frequently (*between-person* correlation).

Within-person processes

On the *within-person* level, we investigate the extent to which *deviations* from individuals' trait levels are related to or even affect each other in the long run. To our knowledge, no study has explicitly investigated such intrapersonal effects. We therefore draw upon our theoretical rationale (outlined earlier) as well as theoretical arguments pertaining to within-person processes in prior research—even if the respective empirical investigation focused on between-person correlations instead. Based on the theoretical rationale for how experiences affect subsequent concerns and behavior—derived from Weinstein (1989), Witte (1998), and Masur (2018)—we argue that experiencing more privacy violations *than usual* (i.e., a person experiences more privacy violations at a certain point in time compared to the amount of privacy violations this person usually experiences) leads to more privacy concerns *than usual* (i.e., a person is more concerned that he or she usually is):

H3a: Individuals who experienced more privacy violations in the last six months than they usually do are subsequently more concerned about privacy than usual (*within-person* correlation).

Likewise, an individual who experiences more privacy violations than usual should subsequently disclose less than usual, because he or she should seek to minimize the risk of again becoming a victim of further privacy violations (cf. Masur, 2018). It is important to note that the direction of the relationship between experiences and disclosure differs depending on whether one focuses on the between- or the within-person level. People who generally disclose frequently also experience more privacy violations, but people who have had more negative privacy experiences *than usual* should subsequently adapt their behavior to prevent future violations. One way of minimizing these risks is to disclose less frequently:

H3b: Individuals who experienced more privacy violations in the last six months than they usually do subsequently disclose personal information online less frequently than they usually do (*within-person* correlation).

Several scholars have argued that the need for privacy may change over time. From a developmental perspective, an individual's understanding and preference for privacy can fluctuate considerably across different stages of the life course

(e.g., Ittelson, Proshansky, Rivlin, & Winkel, 1974; Wolfe & Laufer, 1974; Yao, Rice, & Wallis, 2007). As a person matures, their concept of privacy becomes more cognitively complex (Wolfe & Laufer, 1974). In support of this, age has frequently been found to be a significant predictor of privacy preferences (e.g., Madden, 2012; Rainie, Kiesler, Kang, & Madden, 2013). The need for informational privacy may likewise change over time because individuals develop more privacy literacy and awareness (Büchi et al., 2016; Park, 2013) and mature in their understanding of their privacy needs. Such intraindividual fluctuations in the need for informational privacy should align with variations in people's privacy concerns and privacy-related behavior. We hence hypothesize:

H4a: Individuals who have a higher need for informational privacy than usual are more concerned about privacy than usual (*within-person* correlation).
H4b: Individuals who have a higher need for informational privacy than usual disclose less frequently than usual (*within-person* correlation).

Moderating effects of need for informational privacy

As noted earlier, dispositional need for informational privacy as well as deviations across time should be related to overall privacy concerns and general disclosure frequency as well as deviations in them over time. Person–situation frameworks (cf. Masur, 2018; Rauthmann, Sherman Nave, & Funder, 2015) posit that trait-level factors shape how individuals perceive a certain situation and in turn how such situational perceptions affect behavioral reactions. We thus assume that the need for privacy changes how individuals perceive privacy violations and, in turn, how these transformative experiences affect subsequent concerns and behaviors. If we again distinguish between- and within-person processes, we can identify two types of moderating processes: First, between-person differences in the need for informational privacy could account for how strongly experiences affect subsequent concerns or behaviors at a particular point in time. Individuals who generally do not mind if other people or institutions have access to personal data they disclose in online environments should judge a privacy violation as less severe compared to individuals who feel uncomfortable being fully identifiable (e.g., Trepte & Masur, 2017; Yao, Rice, & Wallis, 2007; Yao & Zhang, 2008):

H5a: A stronger need for informational privacy positively moderates the within-person effect of privacy violation experiences on online privacy concerns (*between-within* interaction).

Second, intraindividual fluctuations in the need for informational privacy could likewise influence the within-person effect of privacy violation experiences on subsequent privacy concerns or information disclosure. More specifically, the effect

may be temporarily stronger among those people who temporarily feel a stronger need for privacy:

H5b: A stronger need for informational privacy negatively moderates the within-person effect of privacy violation experiences on online information disclosure (*between-within* interaction).

On the other hand, within-person deviations from the trait (i.e., a higher or lower need for informational privacy *than usual*) should lead to a stronger or weaker effect of privacy violation experiences on concerns or behaviors at that particular time (Laufer and Wolfe, 1977; Yao, Rice & Wallis, 2007). In other words, privacy violation experiences may only affect people's privacy concerns and disclosure behavior if they feel more in need of informational privacy than usual at that particular time. We hence hypothesize:

H6a: A higher need for informational privacy *than usual* positively moderates the within-person effect of privacy violation experiences on online privacy concerns (*within-within* interaction)
H6b: A higher need for informational privacy *than usual* moderates the within-person effect of privacy violation experiences on online information disclosure (*within-within* interaction).

Method

Sample and procedure

We conducted a five-wave longitudinal panel study from May 2014 to May 2017.[1] We used the same paper-and-pencil questionnaires in each wave to survey a representative sample of the German population (16 years and older). First, a market institute drew a sample of 14,714 potential respondents from a representative omnibus survey (master sample of the Arbeitsgemeinschaft Deutscher Marktforschungsinstitute, ADM) using a random last-two-digit dialing procedure. In this CATI screening, 5,286 respondents agreed to participate in the first three waves. The study was originally designed to be a three-wave panel survey with 6-month intervals, but was extended after the third wave to two more waves at 1-year intervals. 3,278 participants completed the survey at T1. Attrition rates between waves varied between 14.25% and 31.9% ($M = 21.5\%$). In the end, 1,226 participants completed all five waves (Tables S1–S3 in the OSM present sample sizes, attrition rates, and demographic composition at each wave). However, we had to exclude some participants who provided inconsistent birthdates and gender across the study ($n = 45$). The following analyses are based on the subsample of respondents who reported using the Internet at all five waves ($n = 955$). Within this subsample, we excluded participants who did not provide answers to at least half of the items on any of the scales (i.e., systematic missing values; $n = 226$). The final sample thus consisted of 745 respondents ($M_{age} = 55.7$ years old, $SD = 14.3$, range =

16–90; 44.3% female; 61.6% had the highest form of school leaving certificate in Germany). In this subset, the percentage of missing values was 0.21%. All missing values could be considered missing completely at random based on visual inspection of the missingness patterns (see OSM, Figure S2) and the Hawkins and nonparametric tests. Thus, applying a multiple imputation approach, we created four imputed datasets using the bootstrapped expectation-maximization approach implemented in the package *Amelia II* (Honaker & King, 2010), which considers potential time trends in panel data. Although multiple imputation and thus pooling across models is not straightforward when a frequentist approach is applied, it is somewhat trivial when using a Bayesian framework (see below for further information). Pooled results can be achieved by combining the posterior samples of the models estimated on the basis of each imputed dataset.

Measures

This study was part of a larger panel study in which several measures of privacy attitudes, perceptions, and behaviors as well as other psychological concepts were collected.[2] We conducted factor analyses for all latent concepts and evaluated model fit according to the guidelines proposed by Hair, Black, and Rabin (2010, p. 584). After checking factorial validity and reliability, we computed sum or mean scores for each variable. Item formulations, zero-order correlations, and further descriptive analyses can be found in the OSM (Tables S5–S15).

Privacy violation experiences

To assess how often participants had experienced privacy violations, we asked them the following question: "Within the *last 6 months*, how often did you experience the following things on the Internet?" Prior research has identified identity theft, financial fraud, and unwanted sharing of personal information as the most frequently experienced privacy violations (e.g., Chen & Atkin, 2020; Debatin et al., 2009; Trepte, Dienlin, & Reinecke, 2014). We hence presented participants with five items that captured these typical privacy violations (e.g., "Someone else obtained information about you on the Internet that was not meant for this person [e.g. employer, family]"). Participants indicated the frequency with which they had experienced these things in the last 6 months on a 5-point scale ranging from 0 (*never*) to 4 (*four times or more*). Due to the formative nature of this measure, we computed the total number of privacy violation experiences per wave by summing up all five items for each wave ($Ms = 0.29$–0.36, $SDs = 0.83$–0.97).

Half of the participants (51.3%) indicated that they did not experience any of these privacy violations over the course of the study. Furthermore, 17.1% experienced only one and 9.0% only two privacy violations during the five waves of the study. Only 22.6% reported having experienced more than two privacy violations over the course of the entire study. The two most frequently experienced privacy violations were someone else obtaining information about oneself that was not meant for them (e.g., employer, family. . .) and someone else posting pictures of the

respondent on the Internet without their consent. The intraclass correlation coefficient (ICC) revealed considerable within-person changes in experienced privacy violations across the study, because only 39.2% of the total variance could be attributed to between-person differences (ICC = 0.39). Importantly, this measure is *retrospective* because it focuses on people's experiences during the 6 months prior to the actual assessment. In light of this, within-person correlations between experiences and privacy concerns or behaviors can be interpreted as (short-term) longitudinal effects of privacy violation experiences *on* concerns and behaviors. As the following measures of online privacy concerns and online information disclosure assess people's attitudes and behaviors *at each* measurement point, they can be influenced by past experiences, but not vice versa.

Online privacy concerns

Drawing upon prior instruments (e.g., Buchanan, Paine, Joinson, & Reips, 2007), we developed a new scale for measuring privacy concerns on both the vertical level (i.e., with regard to online service providers and governments) and horizontal level (i.e., with regard to other Internet users). We used three items each to measure vertical (e.g., "How concerned are you that institutions or intelligence services will collect and analyze data that you have disclosed on the Internet?") and horizontal privacy concerns (e.g., "How concerned are you that people who you do not know might obtain information about you because of your online activities?"). Respondents indicated their concerns on a 5-point scale ranging from 1 (*not at all concerned*) to 5 (*very concerned*). We tested the factorial validity of the scale using confirmatory factor analysis (CFA). Given the multidimensional structure of the concept, we estimated a second-order factor model for each wave. Factor loadings were constrained to be equal across waves to ensure factorial invariance. The model fit the data well, $\chi^2(345) = 836.11$, $<.001$; CFI = .97; TLI = .96; RMSEA = .05, 90% CI [.04,.05]; SRMR = .04. Comparing this constrained model to an unconstrained model did not reveal a significant difference ($\chi^2(20) = 19.29$, $p = .503$), suggesting that factorial invariance was given for the measure across the five waves. The second-order factor had high reliability, because the proportion of the total score explained by the second-order factor was $\omega_{L1} > 0.85$ in all five waves. McDonald's ω for the subdimensions (horizontal vs. vertical) was between .74 and .89. The average variance extracted was consistently above .52, suggesting good convergent validity. Given the high reliability on the second-order level, we computed mean privacy concerns scores for each wave ($Ms = 3.49$–3.67, $SDs = 0.93$–0.94). Online privacy concerns were relatively stable across the study (ICC = 0.70).

Online information disclosure

In the "Special Eurobarometer" (European Commission, 2015), an ongoing representative survey of the European Union's population with regard to privacy-related topics, online information disclosure is measured by asking respondents to indicate whether they have disclosed certain kinds of information to online shopping and

SNS providers. We assessed online information disclosure in a similar way by asking participants to indicate how often they share certain types of information on the Internet (e.g., first name, last name, financial information, medical information, photos. . .). Respondents indicated the frequency with which they disclosed each item on a 5-point scale ranging from 1 (*never*) to 5 (*daily*). Due to the formative nature of this measure, we computed an overall mean score reflecting the average frequency of disclosing personal information on the Internet ($Ms = 2.17–2.28$, $SDs = 0.58–0.65$). Similar to online privacy concerns, a large share of the variance was explained between-person differences (ICC = 0.61)

Need for informational privacy

We used the first subdimension of the Need for Privacy Questionnaire (Trepte & Masur, 2017), which consists of four items (e.g., "I do not want my personal data to be publicly available" and "Not everyone needs to know everything about me"). Participants answered each item on a 5-point scale ranging from 1 (*do not agree at all*) to 5 (*totally agree*). The scale's factorial validity was tested by computing a unidimensional CFA. Factor loadings were constrained to be equal across waves to ensure factorial invariance. The unidimensional model fit the data well, $\chi^2(132) = 553.67$, $p < .001$; CFI = .94; TLI = .92; RMSEA = .07, 90% CI [.06,.07]; SRMR = .05. Comparing the constrained and unconstrained models yielded a small but significant difference ($\chi^2(12) = 24.03$, $p = .020$). However, given that the constrained model still fits the data well, we concluded that the scale exhibited satisfactory factorial invariance across the five waves. McDonald's ω for the measure was between .85 and .94. The average variance extracted was consistently above .57, suggesting good convergent validity. Need for informational privacy fluctuated considerably across the five waves ($Ms = 4.24–4.32$, $SDs = 0.78–0.84$; ICC = 0.41).

Bayesian estimation framework

We employed a Bayesian estimation framework to test all our hypotheses. In contrast to the frequentist approach, Bayesian estimation derives posterior probability distributions instead of point estimates. Therefore, it allows for assessing not only the most probable value (e.g., the median of the distribution; *Mdn*), but also the probability of any other value (including but not limited to the null value). Following recommendations by Kruschke and Liddell (2018), we did not test whether an effect is "anything-but-null" (i.e., the null hypothesis significance testing approach), but defined ROPE in which the effect size would be deemed negligible. In line with Kruschke and Liddell (2018), we set these ROPEs to range from –0.1 to 0.1 of each standardized dependent variable (as a smaller coefficient would denote a negligible effect size according to Cohen (1988). Hence, the ROPEs differ depending on the dependent variable being considered (online privacy concerns or information disclosure) and whether between- or within-person effects are being estimated. The exact ROPE boundaries for each relationship are listed in Tables 1 and 2. We summarize the posterior distributions using the median (i.e., the most probable

Table 1. Results from the Bayesian Random Effect Within-Between Models Predicting Online Privacy Concerns

	M1								M2							
		90% HDI		ROPE						90% HDI		ROPE				
	Mdn	Lower	Upper	Lower	Upper	%	ESS	Rhat	*Mdn*	Lower	Upper	Lower	Upper	%	ESS	Rhat
(Intercept)	3.63	3.57	3.69	−0.08	0.08	0.00	11,660	1.00	3.63	3.57	3.69	−0.08	0.08	0.00	11,442	1.00
Control variables																
Age	0.01	0.01	0.02	−0.08	0.08	1.00	11,663	1.00	0.01	0.01	0.02	−0.08	0.08	1.00	11,705	1.00
Gender (female)	−0.11	−0.20	−0.02	−0.08	0.08	0.27	11,189	1.00	−0.11	−0.20	−0.02	−0.08	0.08	0.26	11,350	1.00
Education	−0.07	−0.13	−0.01	−0.08	0.08	0.63	11,429	1.00	−0.07	−0.13	−0.01	−0.08	0.08	0.63	11,487	1.00
Exp. of privacy violations																
Between	0.17	0.10	0.24	−0.08	0.08	0.00	13,447	1.00	0.17	0.10	0.24	−0.08	0.08	0.00	12,726	1.00
Within	0.03	0.01	0.05	−0.05	0.05	0.89	7,650	1.01	0.03	0.01	0.05	−0.05	0.05	0.91	14,840	1.01
Need for privacy																
Between	0.58	0.51	0.65	−0.08	0.08	0.00	11,066	1.00	0.58	0.51	0.65	−0.08	0.08	0.00	11,041	1.00
Within	0.08	0.05	0.10	−0.05	0.05	0.00	16,017	1.00	0.08	0.06	0.10	−0.05	0.05	0.00	16,572	1.00
Interactions																
NfP (between) * EoPV (within)									0.00	−0.04	0.03	−0.05	0.05	1.00	16,427	1.01
NfP (within) * EoPV (within)									0.08	0.04	0.12	−0.05	0.05	0.05	17,767	1.00

Note. In Bayesian analyses, posterior probability distributions are obtained instead of point estimates (see also Figure 1). The median (*Mdn*) represents the most probable (or credible) value. The 90% highest posterior density interval (HDI; computed according to Kruschke, 2014, p. 727) provides a range within which the parameters of interest have a 90% probability of falling. The ROPE denotes the range around zero representing negligible effect sizes. % = percentage of the 90% HDI overlapping with ROPE; ESS = effective sample size; Rhat = values close to 1 suggest convergence of the MCMC chains.

Table 2. Results from the Bayesian Random Effect Within-Between Models Predicting Online Information Disclosure

	M3								M4							
		90% HDI		ROPE						90% HDI		ROPE				
	Mdn	Lower	Upper	Lower	Upper	%	ESS	Rhat	*Mdn*	Lower	Upper	Lower	Upper	%	ESS	Rhat
(Intercept)	2.23	2.19	2.27	−0.05	0.05	0.00	10,484	1.00	2.23	2.19	2.27	−0.05	0.05	0.00	11,511	1.00
Control variables																
Age	−0.01	−0.01	0.00	−0.05	0.05	1.00	11,662	1.00	−0.01	−0.01	0.00	−0.05	0.05	1.00	12,269	1.00
Gender (female)	−0.04	−0.10	0.02	−0.05	0.05	0.62	10,312	1.00	−0.04	−0.10	0.02	−0.05	0.05	0.63	10,900	1.00
Education	0.15	0.11	0.19	−0.05	0.05	0.00	10,699	1.00	0.15	0.11	0.19	−0.05	0.05	0.00	11,025	1.00
Exp. of privacy violations																
Between	0.08	0.04	0.13	−0.05	0.05	0.08	11,062	1.00	0.08	0.04	0.13	−0.05	0.05	0.06	11,749	1.00
Within	0.01	0.00	0.03	−0.03	0.03	1.00	16,645	1.00	0.01	0.00	0.03	−0.03	0.03	1.00	16,424	1.00
Need for inf. privacy																
Between	−0.23	−0.28	−0.19	−0.05	0.05	0.00	10,400	1.00	−0.23	−0.28	−0.18	−0.05	0.05	0.00	11,469	1.00
Within	−0.02	−0.04	0.00	−0.03	0.03	0.91	16,225	1.00	−0.02	−0.04	0.00	−0.03	0.03	0.89	17,382	1.00
Interactions																
NfP (between) * EoPV (within)									0.02	−0.01	0.04	−0.03	0.03	0.89	17,237	1.00
NfP (within) * EoPV (within)									−0.04	−0.07	−0.01	−0.03	0.03	0.38	208	1.02

Note. In Bayesian analyses, posterior probability distributions are obtained instead of point estimates (see also Figure 1). The median (*Mdn*) represents the most probable (or credible) value. The 90% highest posterior density interval (HDI; computed according to Kruschke, 2014, p. 727) provides a range within which the parameters of interest have a 90% probability of falling. The ROPE denotes the range around zero representing negligible effect sizes. % = percentage of the 90% HDI overlapping with ROPE; ESS = effective sample size; Rhat = values close to 1 suggest convergence of the MCMC chains.

value) and 90% highest density intervals (HDIs), which indicate which points of the distribution are most credible in the sense that they cover most of the distribution. We consider our hypotheses confirmed if the overlap between the 90% HDIs and the ROPEs is less than 2.5% (Makowski, Ben-Shachar, & Lüdecke, 2019). This is a stricter testing approach than simply testing whether the effect is different from zero, as we effectively test whether the effect is stronger than a specific threshold (i.e., a *small* effect size according to Cohen [1988]).

Data analysis and variable coding

Based on our theoretical reasoning, we sought to separate the between- and within-person variance in the measured variables. This was achieved by analyzing the longitudinal data using the within-between random-effect model (WB-REM; Bell, Fairbrother, & Jones, 2019). Data obtained from longitudinal panel surveys can be regarded as hierarchical because measurements (Level 1) are nested within individuals (Level 2). In a first step, we computed each person's mean on each variable across the five measurement points. In a second step, we computed each person's deviations from these aggregated measures at each measurement point. Finally, using a multilevel modeling approach with random intercepts, we estimated both the between- and within-person effects.

In the absence of an established literature to guide our choice of priors (except for the handful of studies with comparatively small sample sizes), we ran all models using noninformative flat priors (the *brms* default) for all estimated parameters. We estimated two Bayesian linear multilevel regression models for each dependent variable (online privacy concerns and online information disclosure). We first predicted online privacy concerns using privacy violation experiences and the need for informational privacy (Model 1). We then added interactions between (a) privacy violation experiences (within) and need for informational privacy (between) and (b) privacy violation experiences (within) and need for informational privacy (within) (Model 2). Similarly, we first predicted online information disclosure using privacy violation experiences and the need for informational privacy (Model 3), before adding the interactions (Model 4). Prior research has shown that both online privacy concerns and online information disclosure can depend heavily on sociodemographic characteristics (e.g., Madden, 2012; Rainie, Kiesler, Kang, & Madden, 2013). Thus, to account for potential confounds, we included age, gender, and education as control variables in all models.

For each model, we conducted two Markov chain Monte Carlo (MCMC) simulations per imputed dataset, resulting in eight final chains (10,000 iterations each, burn-in periods of 1,000 steps, and a thinning rate of 4).[3] Visual examination of the chain trajectories (see OSM, Figures S3–S6) and Rhat values consistently close to 1 suggested converging results. Posterior predictive checks, which simulate data under the fitted model and then compare these to the observed data, revealed no systematic discrepancies (see OSM, Figures S7–S10).

Results

Between-person differences

H1a predicted a positive between-person relationship between privacy violation experiences and online privacy concerns. The results for the most probable values suggested a small to moderate positive relationship (*Mdn* = 0.17, 90% HDI [0.10,0.24], see Table 1). Furthermore, 0% of the posterior distribution fell inside the ROPE, suggesting a high probability that the effect was greater than "small" (see Figure 1, *upper panel*). Hence, H1a was supported. H1b assumed that privacy violation experiences were positively correlated with online information disclosure. The effect on information disclosure was considerably smaller than the effect on privacy concerns. Although 90% (or 95% respectively) of the posterior distribution did not include zero (*Mdn* = 0.08, 90% HDI [0.04,0.13], see Table 2), 8% of the HDI overlapped with the ROPE. It is thus uncertain whether the effect is large enough to be of theoretical relevance (Figure 1, *lower panel*). Hence, H1b was not supported.

H2a predicted a positive between-person relationship between the need for informational privacy and online privacy concerns. The results revealed a strong positive relationship (*Mdn* = 0.58, 90% HDI [0.51,0.65], 0% in ROPE, see Table 1). Hence,

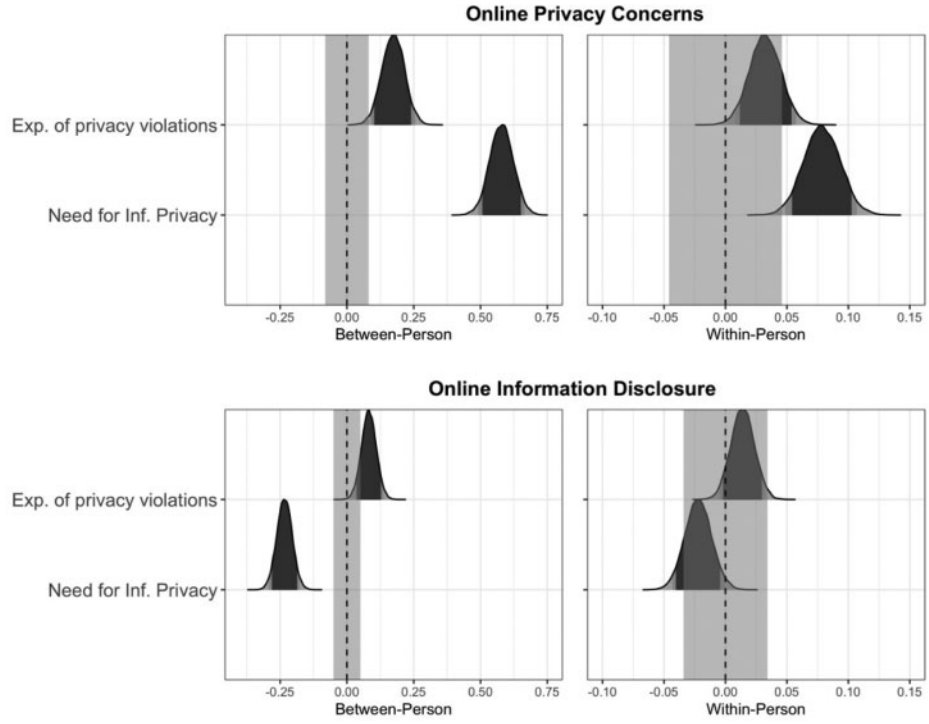

Figure 1 Posterior distributions of Models M1 predicting online privacy concerns (above) and M3 predicting online information disclosure (below). Dark areas represent the 90% HDIs. Gray bars represent ROPEs.

people who generally had a higher need for informational privacy were also generally more concerned about their privacy. Hence, H2a was supported. Furthermore, in line with H2b, we found that a higher need for informational privacy was negatively related to online information disclosure (*Mdn* = –0.23, 90% HDI [–0.28, –0.19], 0% in ROPE, Table 2). People who generally reported having a high need for informational privacy also disclosed less information on average. Hence, H2b was supported.

Within-person processes

H3a argued that a person who experienced more privacy violations than usual in the last 6 months should also exhibit greater privacy concerns than usual. Although 90% (or 95% respectively) of the posterior distribution did not include zero (*Mdn* = 0.03, 90% HDI [0.01, 0.05]), 89% of the HDI overlapped with the ROPE (see Figure 1). Hence, the effect was very small and H3a was not supported. Furthermore, disconfirming H3b, more privacy violation experiences in the last 6 months did not change subsequent disclosure behavior (*Mdn* = 0.01, 90% HDI [0.00, 0.03], 100% in ROPE, see Figure 1 and Table 2].

H4a predicted that people who reported a higher need for informational privacy than usual would also exhibit more privacy concerns than usual. The posterior distribution suggested a small positive correlation (*Mdn* = 0.08, 90% HDI [0.05,0.10], 0% in ROPE, Table 1). Hence, H4a was supported. However, disconfirming H4b, a higher need for informational privacy than usual was not related to deviations in disclosure behavior (*Mdn* = –0.02, 90% HDI [–0.04, 0.00], 91% in ROPE, Table 2).

Moderation analyses

H5a posited that trait need for informational privacy positively moderates the within-person effect of privacy violation experiences on privacy concerns. However, the posterior distributions for the interaction included zero (*Mdn* = 0.00, 90% HDI [–0.04, 0.03]), and the HDI was completely within the ROPE (see Table 1). Hence, H5a was not supported. However, in line with H5b, we found that a higher need for informational privacy than usual positively moderated the within-person effect of privacy violation experiences on online privacy concerns (*Mdn* = 0.08, 90% HDI [0.04, 0.12]). Although the interaction term's HDI overlapped with the ROPE by 5%, the HDI of the within-person effect of privacy violation experiences on concerns fell almost completely outside of the ROPE when the need for informational privacy was one standard deviation higher than usual (*Mdn* = 0.07, 90% HDI [0.04, 0.10], 2% overlap with ROPE; see Figure 2a). This suggests that among people with a higher need for informational privacy than usual, more privacy violation experiences in the last six months positively affected their subsequent online privacy concerns. Hence, H5b was supported.

Disconfirming H6a, trait need for informational privacy did not moderate the within-person effect of experiences on disclosure (*Mdn* = 0.02, 90% HDI [–0.01,

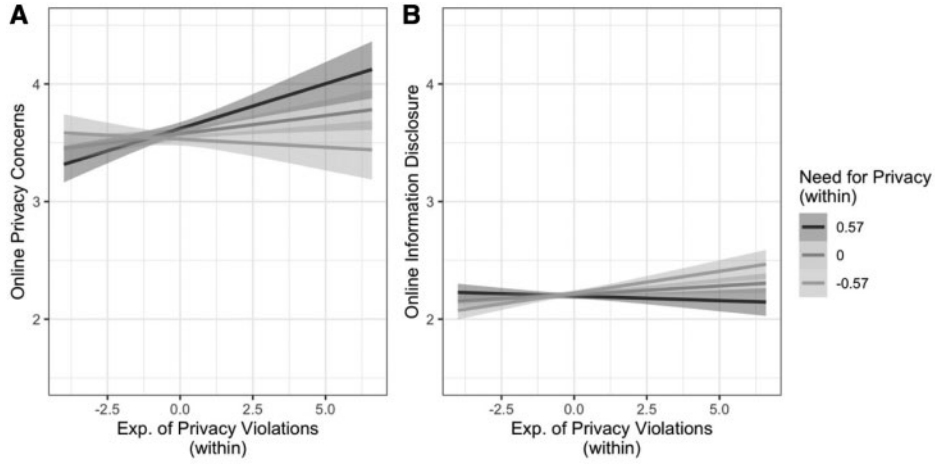

Figure 2 Conditional interaction plots based on Models M2 and M4. (**a**) Moderating effect of need for inf. privacy (within) on the effect of privacy violation experiences (within) on online privacy concerns; (**b**) Moderating effect of need for inf. privacy (within) on the effect of privacy violation experiences (within) on online information disclosure. Need for informational privacy (within) is separated into mean (0) and mean ± SD (±0.57). The dark lines represent the medians of the conditional effect posterior distributions. Transparent areas represent 90% HDIs.

0.04], 89% in ROPE, Table 2). H6b posited that a higher need for informational privacy *than usual* negatively moderates the within-person effect of privacy violation experiences on information disclosure. Although the posterior distribution of the interaction did not include the zero (*Mdn* = –0.04, 90% HDI [–0.07, –0.01]), 38% of the HDI overlapped with the ROPE (Table 2). Based on Figure 2b, it seems that among people who reported a lower need for informational privacy than usual, the most probable within-person effect of privacy violation experiences on information disclosure was positive. However, if such an effect exists, it is probably negligible. Hence, H6b was not supported.

Discussion

In the present study, we extend privacy theory by incorporating privacy violation experiences as antecedents of both online privacy concerns and online information disclosure. We argue that it is important to disentangle between- and within-person processes because a between-person relationship (e.g., people who experience more privacy violations are also more concerned about privacy) does not necessarily imply that experiencing a privacy violation subsequently changes people's concerns or behaviors (within-person effects). Applying a longitudinal panel design with a representative sample, we found a positive between-person relationship between the number of privacy violation experiences and online privacy concerns. On the within-person level, however, we found only small effects of previous privacy

violation experiences on subsequent online privacy concerns and no substantial effects on online information disclosure. These findings suggest that if individuals have more privacy violation experiences than usual, their concerns increase slightly, but only when their need for informational privacy is also higher than usual. A change in subsequent online information disclosure, however, was very improbable. This implies that negative experiences can increase people's online privacy concerns to at least some degree, but might not necessarily change their behavior.

We believe that these results have important implications for future privacy research. Privacy theory and research have long engaged with the fundamental question of how individuals balance their desired and achieved level of access and how this observed (im)balance transforms into behavior (Altman, 1975; Marwick & boyd, 2014; Masur, 2018; Petronio, 2002; Trepte & Reinecke, 2011). When individuals' privacy is violated, a tremendous burden is placed upon them. Such experiences not only shatter subjective conceptions of privacy by violating individually constructed boundaries, but the individual now also has to take this experience into account in all subsequent privacy appraisals and actions. Yet, an important implication of this work is that privacy violations do *not* necessarily result in less information disclosure. We believe that the weak transformative power of privacy violations observed in this study has substantial implications for privacy theory. The general literature on risk perceptions has shown that threat appraisals and responses depend on the severity ascribed to a negative experience and one's perceived efficacy in reacting to it. However, this knowledge has not yet been sufficiently translated into privacy theories and empirical studies (including this study). For example, O'Brien and Mileti (1992) specified that experiencing a natural disaster does not always lead to higher risk perceptions and protective responses. Their findings suggest that if the experienced event did not negatively affect residents, they often thought that they would also be able to avoid the negative consequences of future events. According to Wachinger, Renn, Begg, and Kuhlicke (2013), "this shows that it is less the experience 'in itself,' but rather the severity of the personal consequences experienced in past events that shapes the respondents' perceptions" (p. 1052).

The EPPM similarly suggests that perceived threat and response efficacy are key to determining people's behavioral response (Witte, 1998). In this regard, our findings could be interpreted as follows: Privacy violations that online users frequently experience (and that we were hence able to measure) do not necessarily lead to severe consequences and can often be solved by taking simple corrective measures (e.g., flagging unwanted users, asking other users to delete posts. . .). Furthermore, it is possible that despite appraising such violations as a threat, individuals feel unable to do anything about it. More recent research has shown that the inability to avoid participating in social media and e-commerce and protect one's privacy in all situations and contexts may lead to low self-efficacy and a form of privacy cynicism (Hoffmann, Lutz, & Ranzini, 2016). People may thus engage in fear control strategies such as message avoidance instead of danger control strategies such as active privacy protection or information control (cf. Witte, 1998).

That said, we believe our findings also highlight another gap in the literature: Predominant theories of online privacy often assume that people's privacy behavior is based on rational decision-making. The privacy calculus literature, for example, argues that people's privacy-related behaviors are determined by risk–benefit calculations (Dienlin & Metzger, 2016; Dinev & Hart, 2006). From this perspective, online users might still perceive that the benefits of disclosing information outweigh the risks as predictors of self-disclosure—even when they have actually experienced a privacy violation in the past. However, our results call this rational decision-making procedure into question. The complexity of online environments and the fact that information disclosure is a fundamental driving force of online interactions in both social and commercial contexts may not permit a rational response in the form of protective behavior. To avoid constant deliberation, online users may assess privacy challenges using heuristics rather than elaborate risk–benefit calculations (Metzger & Suh, 2017; Sundar, Kang, Wu, Go, & Zhang, 2013). Users may acknowledge that their online communication behavior encompasses a loss of privacy, but not necessarily experience other severe consequences. They may hence reason based on sunk costs, that is, continue to engage in similar behavior because experiencing harm is inevitable.

Limitations and future perspectives

First, we focused on five rather general examples of online privacy violations that we believed could occur in different online environments. However, there may be more specific privacy violations (or subtler privacy invasions) we neglected in this study. More specifically, our measure reflects privacy violations individuals typically experienced in 2014, when we began the data collection. Since then, new types of violations may have emerged (e.g., unwanted identification by face recognition software; intrusion of insecure Internet of Things [IOT] devices such as smart speakers or connected cars into private spheres such as one's home or car). Qualitative approaches could help to gain a better understanding of what people consider to be a privacy violation today.

Second, what people perceive as a privacy violation may differ depending on the platform being used (e.g., WhatsApp, Facebook, Twitter, health forums. . .), the channel the person is using to communicate (e.g., private message, group chat, public post. . .), their cultural background, or who committed the violation. In our study, we investigated how relatively specific privacy violations affect general privacy concerns and general information disclosure, which could explain the comparatively small effect sizes. Future research should aim to contextualize privacy violations, concerns, and behaviors in order to investigate potential differences across platforms, contexts, and situations.

Third, it is important to consider that within-person relationships may change over time. Changes in personality or disruptive events (e.g., the Snowden revelations or Cambridge Analytica scandal) may change how severely people judge certain privacy violations and whether these experiences affect concerns or behaviors.

Although our study showed no changes in the within-person relationships over the course of the study (bear in mind that privacy violations occurred only very rarely), future investigations should explore whether long-term developments (e.g., experiencing a privacy violation for the first time vs. cumulative experiences) affect the strength of within-person processes.

Fourth, we focused on online information disclosure as behavioral outcome. Although prior work has suggested that managing disclosure behavior in online environments (e.g., minimizing information disclosure) is a form of privacy regulation (Masur & Scharkow, 2016), it nonetheless represents only one way of handling potential risks. Given that the disclosure of personal information is a requirement for most online services, privacy violation experiences might affect people's privacy regulation behavior (e.g., refraining from using certain services, implementing stricter privacy settings, limiting access to disclosures) more than information disclosure itself.

Fifth, and in line with our discussion of Witte's EPPM, it is important to note that we did not investigate whether response efficacy moderates the effect of risk appraisals on subsequent behavior. Future research should take response efficacy into account, as experiences may only affect behavior if perceived efficacy to do something about them is high.

Finally, our study was based on self-reports. However, recall of behaviors can be biased. Even if we would have found an effect of previous experiences on subsequent behaviors, this could also be interpreted as indicating people want to believe they are disclosing less after a privacy violation, even though their actual disclosure behavior has not changed. Future research should aim to employ more objective measures such as tracking individuals' behavior.

Conclusion

Our five-wave panel study revealed that typical privacy violations happen very rarely online. People who experience privacy violations online also report higher privacy concerns compared to those who rarely experience privacy violations online, but do not disclose less. We found that experiencing more than usual violations in the last 6 months slightly increases privacy concerns, but only if the need for informational privacy is simultaneously higher than usual. Unexpectedly, more privacy violation experiences did *not* change subsequent disclosure behavior, not even if the need for informational privacy was higher than usual. Our study therefore suggests that the potential of experiences to transform online communication is less strong than existing theories and findings from primarily cross-sectional studies assume. Future researchers should extend our work by investigating the influence of threat severity, response efficacy (potentially operationalized as privacy self-efficacy and privacy cynicism) on the experience–behavior link and focus on both protection *and* fear control strategies as behavioral outcomes.

We believe that our theoretical analysis and empirical findings further highlight the importance of differentiating between- and within-person associations—

particularly in longitudinal panel studies. Such a distinction allows researchers to align their analyses more closely with theoretical assumptions. This applies not only to research on the effect of privacy violation experiences on subsequent privacy behavior, but to privacy research in general. We thus urge future privacy research to critically address the discrepancy between theoretical within-person reasoning and the predominant empirical strategy of investigating between-person differences.

Supporting Information

Additional Supporting Information may be found in the online version of this article.

Please note: Oxford University Press is not responsible for the content or functionality of any supplementary materials supplied by the authors. Any queries (other than missing material) should be directed to the corresponding author for the article.

Notes

1. A project page on the Open Science Framework (https://osf.io/e8f9v/) includes scripts and reproducible versions of the manuscript and the online supplement document (Online Supplemental Material, OSM) including additional information, tables, figures, and analyses (https://osf.io/d6zse/). The data was published on GESIS Datorium (https://doi.org/10.7802/2117).
2. Other publications linked to the project can be accessed at: https://osf.io/4wabh/
3. Although we simulated eight chains and thus automatically obtained large sample sizes, we nonetheless used 9,000 iterations after warm-up to ensure effective sample sizes close to 10,000 after thinning (following recommendations by Kruschke, 2014). A thinning rate of four was implemented to reduce autocorrelation and increase the efficiency of the chains. In addition to the models reported in the paper, we also estimated models including lagged effects. As they did not fundamentally alter our inferences, they are reported as additional analyses in the OSM (Tables 20 and 21; https://osf.io/d6zse/).

Conflict of Interest

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

Acknowledgments

This research was funded by the German Federal Ministry of Education and Research (BMBF, Funding number: 16KIS0094) awarded to Sabine Trepte.

References

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

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

Awad, N. F., & Krishnan, M. S. (2006). The personalization privacy paradox: An empirical evaluation of information transparency and the willingness to be profiled online for personalization. *Mis Quarterly*, 30, 13–28. https://doi.org/10.5555/2017284.2017287

Bansal, G., Zahedi, F. , & Gefen, D. (2007). The impact of personal dispositions on privacy and trust in disclosing health information online. *AMCIS 2007 Proceedings*, 57. Retrieved from http://aisel.aisnet.org/amcis2007/57

Baruh, L., & Popescu, M. (2017). Big data analytics and the limits of privacy self-management. *New Media & Society*, 19, 579–596. https://doi.org/10.1177/1461444815614001

Bayer, J. B., Triệu, P., & Ellison, N. B. (2020). Social media elements, ecologies, and effects. *Annual Review of Psychology*, 71(1), 471–497. https://doi.org/10.1146/annurev-psych-010419-050944

Bélanger, F., & Crossler, R. E. (2011). Privacy in the digital age: A review of information privacy research in information systems. *MIS Quarterly*, 35, 1017–1041.

Bell, A., Fairbrother, M., & Jones, K. (2019). Fixed and random effects models: Making an informed choice. *Quality & Quantity*, 53, 1051–1074. https://doi.org/10.1007/s11135-018-0802-x

boyd, d. (2008). Why youth (heart) social network sites: The role of networked publics in teenage social life. In D. Buckingham (Ed.), *Youth, identity, and digital media* (pp. 119–142). Cambridge, MA: MIT Press.

Buchanan, T., Paine, C., Joinson, A. N., & Reips, U.-D. (2007). Development of measures of online privacy concern and protection for use on the internet. *Journal of the American Society for Information Science and Technology*, 58, 157–165. https://doi.org/10.1002/asi.20459

Büchi, M., Just, N., & Latzer, M. (2016). Caring is not enough: The importance of Internet skills for online privacy protection. *Information, Communication & Society*, 20, 1261–1278. https://doi.org/10.1080/1369118X.2016.1229001

Chen, H., & Atkin, D. (2020). Understanding third-person perception about Internet privacy risks. *New Media & Society*, 1–19. https://doi.org/10.1177/1461444820902103

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, 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. B. Wright & L. M. Webb (Eds.), *Computer-mediated communication in personal relationships* (pp. 21–40). New York, NY: Peter Lang.

Choi, Y. H., & Bazarova, N. N. (2014). Self-Disclosure in social media: Extending the functional approach to disclosure motivations and characteristics on social network sites. *Journal of Communication*, 64, 635–657. https://doi.org/10.1111/jcom.12106

Cohen J. 1988. *Statistical power analysis for the behavioral sciences*. (2nd ed.). Hillsdale, NJ. Erlbaum.

Debatin, B., Lovejoy, J. P., Horn, A. K., & Hughes, B. N. (2009). Facebook and online privacy: Attitudes, behaviors, and unintended consequences. *Journal of Computer-Mediated Communication*, 15, 83–108. https://doi.org/10.1111/j.1083-6101.2009.01494.x

Dienlin, T., Masur, P. K., & Trepte, S. (2019). A longitudinal analysis of the privacy paradox. *SocArXiv*. https://doi.org/10.31235/osf.io/fm4h7

Dienlin, T., & Metzger, M. J. (2016). An extended privacy calculus model for SNSs—Analyzing self-disclosure and self-withdrawal in a U.S. Representative sample. *Journal of Computer-Mediated Communication*, 21, 368–383. doi: https://doi.org/10.1111/jcc4.12163

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

European Commission. (2015). *Special Eurobarometer 431: Data protection*. Brussels, BE. Retrieved from http://ec.europa.eu/public_opinion/archives/ebs/ebs_431_en.pdf

Greenwald, G. (2014). *No place to hide: Edward Snowden, the NSA and the surveillance state*. London: Hamish Hamilton.

Hamaker, E. L., Kuiper, R. M., & Grasman, R. P. P. P. (2015). A critique of the cross-lagged panel model. *Psychological Methods*, 20, 102–116. https://doi.org/10.1037/a0038889

Honaker, J., & King, G. (2010). What to do about missing values in time series cross-section data. *America Journal of Political Science*, 54, 561–581.

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

Ittelson, W., Proshansky, H., Rivlin, L., & Winkel, G. (1974). *An introduction to environmental psychology*. Oxford, England: Holt, Rinehart &Winston.

Janoff-Bulmann, R., & Schwartzberg, S. (1991). Toward a general model of personal change. In C. R. Snyder & D. Forsyth (Eds.), *Handbook of social and clinical psychology: The health perspective* (pp. 488–508). New York: Pergamon.

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://doi.org/10.1109/HICSS.2010.307

Kruschke, J. K. (2014). *Doing Bayesian data analysis: A tutorial for R, JAGS, and Stan*. New York: Academic Press.

Kruschke, J. K., & Liddell, T. M. (2018). The Bayesian new statistics: Hypothesis testing, estimation, meta-analysis, and power analysis from a Bayesian perspective. *Psychonomic Bulletin & Review*, 25, 178–206. https://doi.org/10.3758/s13423-016-1221-4

Laufer R. S. & Wolfe M. (1977). Privacy as a concept and social issue: A multidimensional developmental theory. *Journal of Social Issues,* 33(3), 22–42.

Keijsers, L., Voelkle, M. C., Maciejewski, D., Branje, S., Koot, H., Hiemstra, M., & Meeus, W. (2016). What drives developmental change in adolescent disclosure and maternal knowledge? Heterogeneity in within-family processes. *Developmental Psychology*, 52, 2057–2070. https://doi.org/10.1037/dev0000220

Loewenstein, G. F., Weber, E. U., Hsee, C. K., & Welch, N. (2001). Risk as feelings. *Psychological Bulletin*, 127, 267–286.

Madden, M. (2012). *Privacy management on social media sites.* Retrieved from https://www.pewresearch.org/internet/2012/02/24/privacy-management-on-social-media-sites/

Makowski, D., Ben-Shachar, M., Lüdecke, D. (2019). bayestestR: Describing effects and their uncertainty, existence and significance within the Bayesian Framework. *Journal of Open Source Software*, 4, 1541. https://joss.theoj.org/papers/10.21105/joss.01541.

Marwick, A. E., & Boyd, D. (2014). Networked privacy: How teenagers negotiate context in social media. *New Media & Society*, 16, 1051–1067. https://doi.org/10.1177/1461444814543995

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

Masur, P. K., & Scharkow, M. (2016). Disclosure management on social network sites: Individual privacy perceptions and user-directed privacy strategies. *Social Media + Society*, 1–13. https://doi.org/10.1177/2056305116634368

Matzner, T., Masur, P. K., Ochs, C., & Pape, T. von. (2016). Do-it-yourself data protection—Empowerment or burden? In S. Gutwirth, R. Leenes, & P. De Hert (Eds.), *Data protection on the move: Current developments in ICT and privacy/data protection* (pp. 277–305). Dordrecht: Springer Netherlands.

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

Nissenbaum, H. (2010). *Privacy in context: Technology, policy, and the integrity of social life*. Palo Alto, CA: Stanford University Press.

O'Brien, P. W., & Mileti, D. S. (1992). *Public response to aftershock warnings*. Fort Collins, Co: Colorado State University.

Papacharissi, Z. (2010). *A private sphere: Democracy in a digital age*. Cambridge: Polity Press.

Park, Y. J. (2013). Digital literacy and privacy behavior online. *Communication Research*, 40, 215–236. https://doi.org/101177/0093650211418338

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

Popova, L. (2012). The extended parallel process model: Illuminating the gaps in research. *Health Education & Behavior*, 39, 455–473. https://doi.org/10.1177/1090198111418108

Rainie, L., Kiesler, S., Kang, R., & Madden, M. (2013). *Anonymity, privacy, and security online.* Retrieved from https://www.pewresearch.org/internet/2013/09/05/part-1-the-quest-for-anonymity-online/

Rauthmann, J. F., Sherman, R. A., Nave, C. S., & Funder, D. C. (2015). Personality-driven situation experience, contact, and construal: How people's personality traits predict characteristics of their situations in daily life. *Journal of Research in Personality*, 55, 98–111. https://doi.org/101016/j.jrp.2015.02.003

Smith, H. J., Milberg, S. J., & Burke, S. J. (1996). Information privacy: Measuring individual's concerns about organizational practices. *MIS Quarterly*, 20, 167–196. https://doi.org/10.2307/249477

Solove, D. J. (2004). *The digital person: Technology and privacy in the information age*. New York: NYU Press.

Sundar, S. S., Kang, H., Wu, M., Go, E., & Zhang, B. (2013). Unlocking the privacy paradox: Do cognitive heuristics hold the key? In P. Baudisch, M. Beaudouin-Lafon & W. E. Mackay (Eds.), *CHI '13 extended abstracts on human factors in computing systems* (pp. 811–816). New York, NY: Association for Computing Machinery. https://doi.org/10.1145/2468356.2468501

Trepte S. & Masur P. K. (2017). The need for privacy. In: V. V. Zeigler-Hill & T. K. Shackelford (Eds.), *Encyclopedia of personality and individual differences*. London: Springer.

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

Trepte, S., Dienlin, T., & Reinecke, L. (2014). Risky behaviors: How online experiences influence privacy behaviors. In B. Stark, O. Quiring, & N. Jackob (Eds.), *Von der Gutenberg-Galaxis zur Google-Galaxis* (Vol. 41, pp. 225–244). Konstanz: UVK.

Trepte, S. & Reinecke, L. (2011). *Privacy online: Perspectives on privacy and self-disclosure*. Berlin: Springer.

Voelkle, M. C., Brose, A., Schmiedek, F., & Lindenberger, U. (2014). Toward a unified framework for the study of between-person and within-person structures: Building a bridge between two research paradigms. *Multivariate Behavioral Research*, 49, 193–213. https://doi.org/10.1080/00273171.2014.889593

Wachinger, G., Renn, O., Begg, C., & Kuhlicke, C. (2013). The risk perception paradox–implications for governance and communication of natural hazards. *Risk Analysis: An Official Publication of the Society for Risk Analysis*, 33, 1049–1065. https://doi.org/10.1111/j.1539-6924.2012.01942.x

Weinstein, N. D. (1989). Effects of personal experience on self-protective behavior. *Psychological Bulletin*, 105, 31–50. https://doi.org/10.1037/0033-2909.105.1.31

Witte, K. (1998). Fear as motivator, fear as inhibitor: Using the extended parallel process model to explain fear appeal successes and failures. In P. A. Andersen & L. K. Guerrero (Eds.), *Handbook of communication and emotion: Research, theory, applications, and contexts* (pp. 423–450). San Diego, CA: Academic Press.

Wolfe, M., & Laufer, R. (1974). The concept of privacy in childhood and adolescence. In S. T. Margulis (Ed.), *Privacy* (pp. 29–54). Stroudsburg, PA: Dowden, Hutchinson & Ross.

van der Sloot, B., & de Groot, A. (2018). *The handbook of privacy studies: An interdisciplinary introduction*. Amsterdam: Amsterdam University Press.

Xu, H., Teo, H.-H., Tan, B. C. Y., & Agarwal, R. (2012). Research note—Effects of individual self-protection, industry self-regulation, and government regulation on privacy concerns: A study of location-based services. *Information Systems Research*, 23, 1342–1363. https://doi.org/10.1287/isre.1120.0416

Yao, M. Z., & Linz, D. G. (2008). Predicting self-protections of online privacy. *CyberPsychology & Behavior*, 11, 615–617. https://doi.org/10.1089/cpb.2007.0208

Yao, M. Z, Rice, R. E., & Wallis, K. (2007). Predicting user concerns about online privacy. *Journal of the American Society for Information Science and Technology*, 58, 710–722.

Yao, M. Z., & Zhang, J. (2007). Predicting user concerns about online privacy in Hong Kong. *CyberPsychology & Behavior*, 11, 779–781. https://doi.org/10.1089/cpb.2007.0252