Do Likes Buttons Increase Self-Disclosure? Analyzing how Online Communication is Affected by Popularity Cues Using the Privacy Calculus Model

Abstract

How do like and dislike buttons affect online communication? According to the privacy calculus model, online self-disclosure is determined by privacy concerns and expected benefits. It seems possible that like and dislike buttons affect self-disclosure, for example because they increase expected benefits or privacy concerns. To find out, we conducted a preregistered one-week field experiment. Participants were randomly distributed to three different websites, on which they discussed a current political topic. The websites featured either (a) like buttons, (b) like and dislike buttons, or (c) no like or dislike buttons. The final sample consisted of 590 participants. The results showed that the mere existence of a like and dislike button did not affect online communication. Self-disclosure could be predicted successfully using the privacy calculus variables.

Keywords: privacy calculus, communication, popularity cues, field experiment, structural equation modeling, preregistration

Word count: 6073

Do Likes Buttons Increase Self-Disclosure? Analyzing how Online Communication is Affected by Popularity Cues Using the Privacy Calculus Model

Introduction

Understanding why people share personal information online is a critical question for society and research. Originally, it was assumed that the online sharing of information is erratic and that it cannot be predicted by people's personal beliefs, concerns, or attitudes. Most prominently, the privacy paradox stated that people communicate vast amounts of personal information online *despite* having substantial concerns about their privacy (Barnes, 2006; Taddicken & Jers, 2011).

Somewhat surprisingly, and despite its popularity in the media (New York Public Radio, 2018), empirical support for the privacy paradox is ambivalent.

A recent meta-analysis reported a correlation between privacy concerns and self-disclosure on SNS of r = -.13 (Baruh, Secinti, & Cemalcilar, 2017), which shows that privacy concerns are indeed related to communication online.

Rather than further pursuing the privacy paradox, a large share of current day research builds on the so-called *privacy-calculus* (Laufer & Wolfe, 1977). The privacy calculus states that communication online can be explained—at least partly—by means of expected risks *and* expected benefits (Krasnova, Spiekermann, Koroleva, & Hildebrand, 2010). By operationalizing expected risks as privacy concerns, several studies have shown that experiencing privacy concerns is related to sharing less information online, whereas expecting benefits is related to sharing more information online (Heirman, Walrave, & Ponnet, 2013; Koohikamali, French, & Kim, 2019).

However, although the privacy calculus has gained momentum in academic research, several important questions remain unanswered.

First, current research on the privacy calculus is often criticized for not explicitly focusing on the *deliberation process* when communicating online. According to critics (e.g., Knijnenburg et al., 2017), showing that both concerns and gratifications correlate with communication behavior online is not sufficient evidence for an explicit weighing process. This study, therefore, explicitly focuses on the privacy deliberation process.

Second, in this study I approach the privacy calculus from a theoretical perspective of *bounded rationality*. It is likely that other factors next to risks and benefits also determine behavior. I therefore extend the privacy calculus model theoretically by investigating the role and interplay of trust and self-efficacy.

Third, the privacy calculus does not take place in a vacuum. It is often argued that communication online can be easily triggered by external circumstances. I therefore analyze whether the privacy calculus is affected by the affordances of a website. Specifically, I investigate whether *popularity cues* such as like and dislike buttons affect the privacy calculus and whether they foster communication online.

Fourth, it is still largely unknown whether the privacy calculus can be replicated with *behavioral data* in an authentic long-term setting (Kokolakis, 2017). Thus far, much research on the privacy calculus used self-reports of behavior (Krasnova et al., 2010), vignette approaches (Bol et al., 2018), or one-shot experiments in the lab (Trepte, Scharkow, & Dienlin, 2020). A long-term field study observing actual behavior in an authentic context is still missing.

To test the research questions, a representative sample of the German population was collected in a preregistered online field experiment. Participants were randomly distributed to one of three different websites, which either included a like button, both a like and a dislike button, or no buttons at all. Over the course of one week, participants had the chance to discuss a topical issue (i.e., prevention of terrorist attacks in Germany). Afterward, they answered a follow-up questionnaire with items measuring the privacy calculus variables.

The Privacy Calculus

The key variable of interest for this study is (verbal) communication online. Are people willing to engage in a conversation? Do they express their opinion? In communicating online, people share much information about themselves. Communication is, hence, closely related to self-disclosure, and it is a primary means of regulating privacy (e.g., Dienlin, 2014).

Privacy concerns were defined as follows. "Taken together, concerns about online privacy represent how much an individual is motivated to focus on their control over a voluntary withdrawal from other people or societal institutions on the Internet, accompanied by an uneasy feeling that their privacy might be threatened" (Dienlin, Masur, & Trepte, 2021, p. 4).

In this study I adopt the theoretical perspective of the privacy calculus (Laufer & Wolfe, 1977). The privacy calculus assumes that when communicating online people engage in a rational weighing of risks and benefits. Notably, I don't assume that this weighing process is flawless or that humans are perfect rational agents. Instead, I understand the privacy calculus from the perspective of *bounded rationality* (Simon, 1990). Bounded rationality has three tenets: "(1) humans are cognitively constrained; (2) these constraints impact decision making; and (3) difficult problems reveal the constraints and highlight their significance." (Bendor, 2015, p. 1303) Crucially, although bounded rationally upholds that human behavior is not perfectly logical, this does not meant that it is irrational (Gigerenzer, Selten, & Workshop, 2002). Instead, it is a continuum. Humans are still trying to optimize the outcomes of their behavior according to their own best interests or values. It is only that their capacity to do so is bounded.

Transferred to the context of online privacy, it is by now well known that several irregularities and inconsistencies between concerns and communication behavior exist. These differences stem from, for example, information asymmetries, present bias, intangibility, illusory control, or herding (Acquisti, Brandimarte, & Loewenstein, 2020). At the same time, *on average* people do behave according to their interests, respond to incentives, or actively manage their privacy (Baruh et al., 2017; Dienlin & Metzger, 2016; Solove, 2020).

I therefore hypothesize that people who experience more privacy concerns engage in less communication online. In light of bounded rationality and the existence of other competing factors that also influence online-communication (see below), the effect is likely small.

In turn, the most relevant factor driving online communication is *expected gratifications*. People accept a loss of privacy if they can gain something in return (e.g., Laufer & Wolfe, 1977). The most prominent gratifications of online communication include social support (Krasnova et al., 2010), social capital (Ellison, Vitak, Steinfield, Gray, & Lampe, 2011), entertainment (Dhir & Tsai, 2017), information-seeking (Whiting & Williams, 2013), and self-presentation (Min & Kim, 2015). Several studies have shown, that gratifications outweigh concerns (Bol et al., 2018; Dienlin & Metzger, 2016). As a result, we expect a moderate relationship.

H1: People who are more concerned about their privacy than others are less likely to communicate actively on a website.

H2: People who obtain more gratifications from using a website are more likely to communicate actively on a website.

Privacy calculus implies that people *explicitly* compare benefits and disadvantages before communicating online. Research on the privacy calculus has often ignored this aspect (Knijnenburg et al., 2017). Only observing that privacy concerns or expected gratifications and communication online are *related* is insufficient to prove an explicit weighing process. Hence, we here analyze how much people actively deliberate about their privacy and how that might influence the privacy calculus.

We can understand the privacy calculus from two perspectives (Table **??**): First, is the communication behavior aligned with people's privacy concerns and expected benefits?

Second, is the communication process implicit or explicit?

Here, I suggest that the privacy calculus should be discussed in light of dual process theories, which state that people either deliberately, explicitly, and centrally take decisions, or instead do so automatically, implicitly, and peripherally (Kahneman, 2011; Petty & Cacioppo, 1986). Accordingly, privacy calculus would assume that people, when it comes to disclosing, engage in a central processing. Building on Omarzu (2000) and Altman (1976), I hence introduce and investigate a novel concept termed *privacy deliberation*. Privacy deliberation captures the extent to which individual people explicitly compare potential positive and negative outcomes before communicating with others.

On the one hand, deliberating about privacy could *reduce* subsequent communication. Refraining from communication—the primary means of connecting with others—likely requires some active and deliberate restraint. This is especially true for social media, which are designed to elicit communication and participation. Actively thinking about whether communicating is really worthwhile might be the first step not to participate. On the other hand, deliberating about privacy might also *increase* communication. A person concerned about their privacy might conclude that in this situation communication is actually beneficial. Deliberation could represent some kind of inner consent, providing additional affirmation.

Alternatively, it could be that deliberation functions as a moderator. For example, if people actively deliberate about whether or not to disclose, this might reinforce the effect of concerns or gratifications. Reflecting about the pros and cons of communication might concerns and gratifications more salient. Alternatively, it could also be that deliberating decreases the effects, for example because apparent gratifications are considered more critically, and maybe loose their appeal.

I therefore formulate the following two research questions:

RQ1: Do people who deliberate more actively whether they should communicate, communicate more or less online?

RQ2: Do people who deliberate more actively whether they should communicate, show larger or smaller relations between concerns, gratifications and communication behavior?

Bounded rationality implies that additional factors should also explain communication. Communication online often takes place in situations where information is limited or obscure. The more familiar users are with a context, the more experience, knowledge, and literacy they possess, the more likely they should be to navigate online contexts successfully. In other words, if users possess more *self-efficacy* to participate, they should also communicate more. Related, people who report more privacy self-efficacy also engage in more self-withdrawal (Chen, 2018; Dienlin & Metzger, 2016).

H3: People are more likely to communicate on a website when their self-efficacy about self-disclosing on the website is higher.

In situations where people lack experience or competence, the most relevant variable explaining behavior is, arguably, *trust*. Online, users often cannot control the context or the way their information is handled. Trust therefore plays a key role in online communication (Metzger, 2004). People who put more trust in the providers of networks, for example, disclose more personal information (Li, 2011).

Trust can be conceptualized in two different ways (Gefen, Karahanna, & Straub, 2003). It either captures "*specific* beliefs dealing primarily with the integrity, benevolence, and ability of another party" (Gefen et al., 2003, p. 55, emphasis added). Alternatively, it refers to a "*general* belief that another party can be trusted" (Gefen et al., 2003, p. 55, emphasis added). Whereas specific trust focuses on the causes of trust, general trust emphasizes the experience of trust. In the online context, there exist several different *targets* of trust, including (a) the information system, (b) the provider, (c) the Internet, and (d) the community of other users (Söllner, Hoffmann, & Leimeister, 2016). Because the targets can be largely different, it is often recommended to analyze them individually.

H4: People are more likely to communicate on a website when they have greater trust in the provider, the website, and the other users.

The Effect of Popularity Cues

So far I analyzed user-oriented factors that explain communication online. But how does the context, the digital infrastructure, affect the privacy calculus and communication? In what follows I do not focus on specific *features* of particular websites, which can change and quickly become obsolete (Fox & McEwan, 2017). Instead, I address the underlying latent structures by analyzing so-called *affordances* (Ellison & Vitak, 2015; Fox & McEwan, 2017). Developed by Gibson (2015), affordances emphasize that it is not the *objective features* of objects that determine behavior, but rather our *subjective perceptions.* Affordances are mental representations of how objects might be used. There is an ongoing debate on what exactly defines an affordance (Evans, Pearce, Vitak, & Treem, 2017). For example, whereas Evans et al. (2017) propose three affordances for mediated communication (i.e., anonymity, persistence, and visibility), Fox and McEwan (2017) suggest 10 affordances for SNSs alone (i.e., accessibility, bandwidth, social presence, privacy, network association, personalization, persistence, editability, conversation control, and anonymity).

The privacy calculus states that both benefits and costs determine behavior. Popularity cues such as like and dislike buttons, which are categorized as "paralinguistic digital affordances" (Carr, Hayes, & Sumner, 2018, p. 142), can be linked to the two sides of the privacy calculus. The like button is positive and a potential benefit: It expresses an endorsement, a compliment, a reward (Carr et al., 2018; Sumner, Ruge-Jones, & Alcorn, 2017). The dislike button is negative and a potential cost: It expresses criticism and a way to downgrade content.

Paralinguistic digital affordances and specifically popularity cues can affect behavior (Krämer & Schäwel, 2020; Trepte et al., 2020). Online comments that already have several dislikes are much more likely to receive further dislikes (Muchnik, Aral, & Taylor, 2013).

When users disagree with a post, they are more likely to click on a button labeled *respect* compared to a button labeled *like* (Stroud, Muddiman, & Scacco, 2017). The potentially stark negative effect of the dislike button might also explain why to date only a handful of major websites have implemented it (e.g., youtube, reddit, or stackexchange). In this vein, popularity cues likely also impact the privacy calculus (Krämer & Schäwel, 2020).

Specifically, *likes* are positive and represent the positivity bias typical of social media (Reinecke & Trepte, 2014). Receiving a like online is similar to receiving a compliment offline. Introducing like-buttons mighty afford and emphasize a *gain frame* (Rosoff, Cui, & John, 2013). These gains can be garnered only through participation. Because like buttons emphasize positive outcomes, it is likely that concerns decrease. In situations where there is more to win, people should also more actively deliberate about whether or not to disclose information.

Receiving a *dislike* should feel more like a punishment. Dislikes introduce a *loss frame*. As a result, websites featuring both like *and* dislike buttons should be more ambivalent compared to websites without any popularity cues. In online contexts, gains often outweigh losses. Having both types of popularity cues might still lead to more gratifications and communication. However, privacy concerns should not be reduced anymore: People who are more concerned about their privacy are also more shy and risk averse (Dienlin, 2017). Implementing the dislike button might therefore increase privacy concerns, thereby canceling out the positive effects of the like button. And because there is more at stake, participants should deliberate even more whether or not to disclose.

There are two potential underlying theoretical pathways: The *mere presence* of popularity cues might affect whether people are willing to disclose; being able to attract likes might motivate users to communicate, while the mere option to receive dislikes might intimidate others. On the other hand, *actually receiving* likes or dislikes might then affect subsequent behavior, potentially reinforcing the process.

H5. Compared to people who use a website without like or dislike buttons, people who use a website with like buttons (a) communicate more, (b) obtain more gratifications, (c) are less concerned about their privacy, and (d) deliberate more about whether they should communicate online.

H6. Compared to people who use a website without like or dislike buttons, people who use a website with like *and* dislike buttons (a) communicate more, (b) obtain more gratifications, and (c) deliberate more about whether they should communicate online.

H7. Compared to people who use a website with only like buttons, people who use a website with like and dislike buttons (a) are more concerned about their privacy, and (b) deliberate more about whether they should communicate online.

For a simplified overview of the analyzed model, see Figure 1.

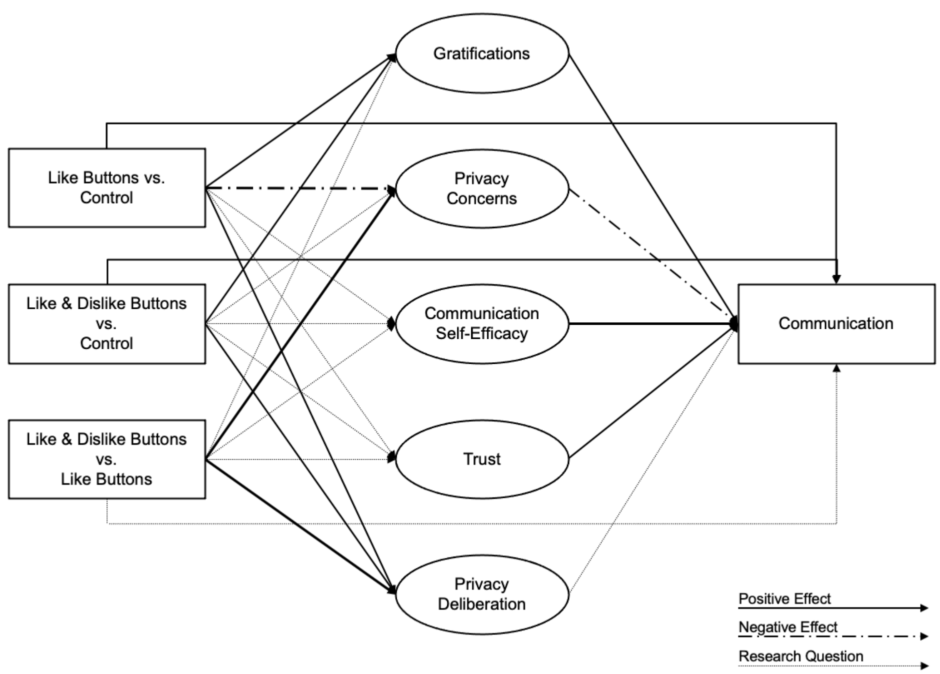

Figure 1. Overview of analyzed model.

Methods

Open Science

The online supplementary material (OSM) of this study includes the data, research materials, analyses scripts, and a reproducible version of this manuscript, which can be found on the manuscript's companion website (https://XMtRa.github.io/privacy_calc_exp_anon). I preregistered the study using the registration form *OSF Prereg*, which includes the hypotheses, sample size, research materials, analyses, and exclusion criteria (see https://osf.io/a6tzc/?view_only=5d0ef9fe5e1745878cd1b19273cdf859). I needed to change the pre-defined plan in some cases. For a full account of all changes, see OSM. New analyses that were not preregistered appear in the section Exploratory Analyses.

Procedure

The study was designed as an online field experiment with three different groups. The first group used a website without like or dislike buttons, the second the same website but with only like buttons, and the third the same website but with both like and dislike buttons. Participants were randomly distributed to one of the three websites in a between-subject design.

I collaborated with a market research company to recruit participants. As incentive, participants were awarded digital points, which they could use to get special offers from other online commerce services. Participants were above the age of 18 and lived in Germany. In a first step, the company sent its panel members an invitation to participate in the study (*invitation*). In this invitation, panel members were asked to participate in a study analyzing the current threat posed by terrorist attacks in Germany.[1] Members who

[1] Although the terror attack was not of primary interest for this study, the data can and will also be used to analyze perceptions of the terrorism threat. Hence, no deception took place, and in the debriefing participants were informed about the additional research interest in privacy.

decided to take part were subsequently sent the first questionnaire (*T1*), in which I (a) asked about their sociodemographics, (b) provided more details about the study, and (c) included a registration link for the website, which was described as "participation platform". Afterward, participants were randomly assigned to one of the three websites. After registration was completed, participants were invited (but not obliged) to discuss the topic of the terrorism threat in Germany over the course of one week (*field*). Subsequently, participants received a follow-up questionnaire in which the self-reported measures were collected (*T2*). Measures were collected after and not before the field phase in order not to prime participants or reveal the primary research interest.

The online website was programmed based on the open-source software *discourse* (https://www.discourse.org/). I conducted several pretests with students from the local university to make sure the website had an authentic feel (see Figure 2). Nine hundred sixty participants created a user account on the website (see below) and used the website actively. Overall, they spent 162 hours online, wrote 1,171 comments, and clicked on 560 popularity cues. Notably, there were no instances of people providing meaningless text. For an example of communication that took place, see Figure 3.

Participants

I ran a priori power analyses to determine sample size. The power analysis was based on a smallest effect size of interest [SESOI; Lakens, Scheel, and Isager (2018)]. Namely, I defined a minimum effect size considered sufficiently large to support the hypotheses. Because small effects should be expected when researching aspects of privacy online (e.g., Baruh et al., 2017), with standardized small effects beginning at an effect size of $r = .10$ (Cohen, 1992), I set the SESOI to be $r = .10$. The aim was to be able to detect this SESOI with a probability of at least 95%. Using the regular alpha level of 5%, basic power analyses revealed a minimum sample size of N = 1,077. In the end, I was able to include N = 559 in the analyses (see below). This means that the study had a probability (power) of

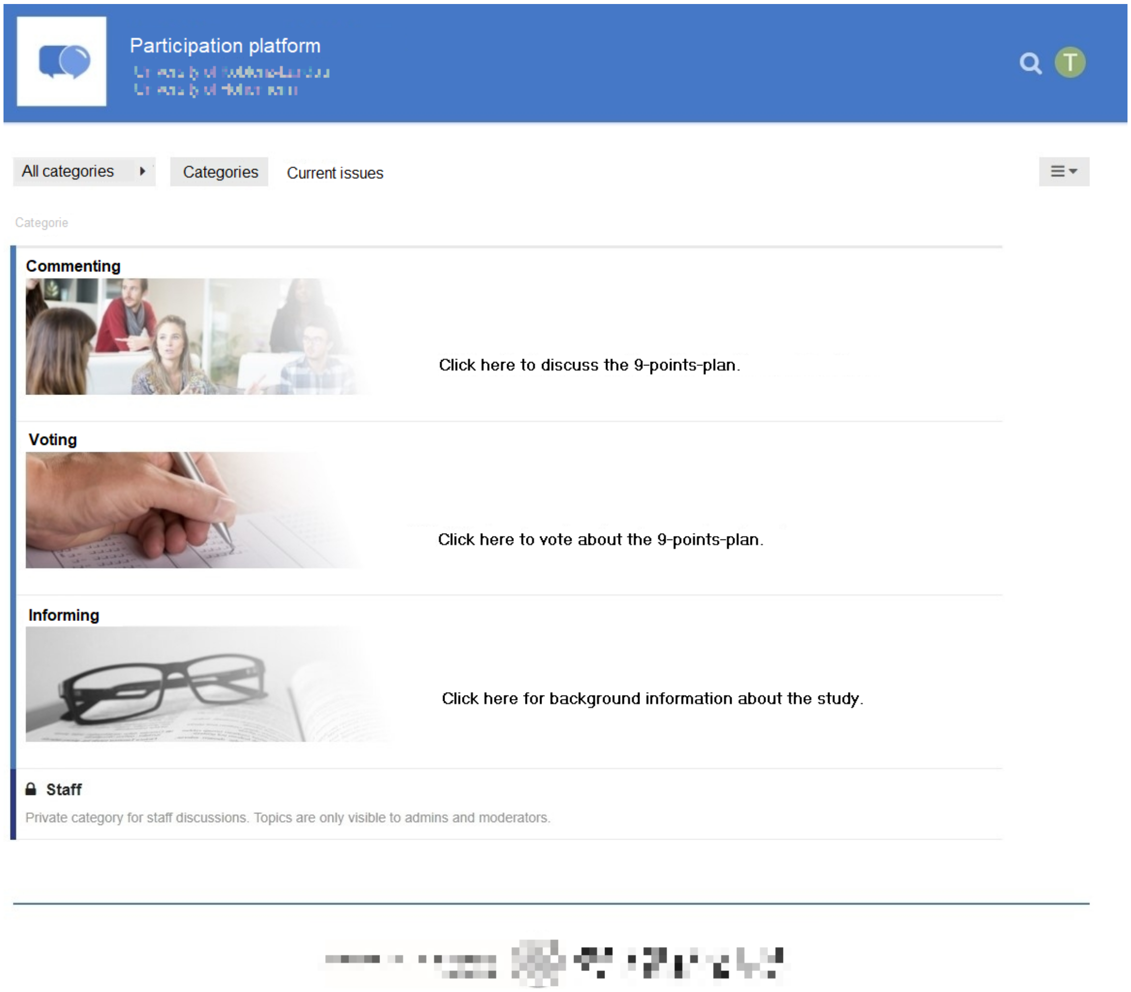

Figure 2. The website's homepage. (Translated to English.)

77% to find an effect at least as large as $r = .10$. Put differently, I was able to make reliable inferences (i.e., power = 95%) about effects at least as big as $r = .14$.

A representative sample of the German population in terms of age, sex, and federal state was collected. In sum, 1,619 participants completed the survey at T1, 960 participants created a user account on the website, and 982 participants completed the survey at T2. Using tokens and IP addresses, I connected the data from T1, participants' behavior on the website, and T2 by means of objective and automated processes. The data of several participants could not be matched for technical reasons, for example because they used different devices for the respective steps. In the end, the data of 590 participants

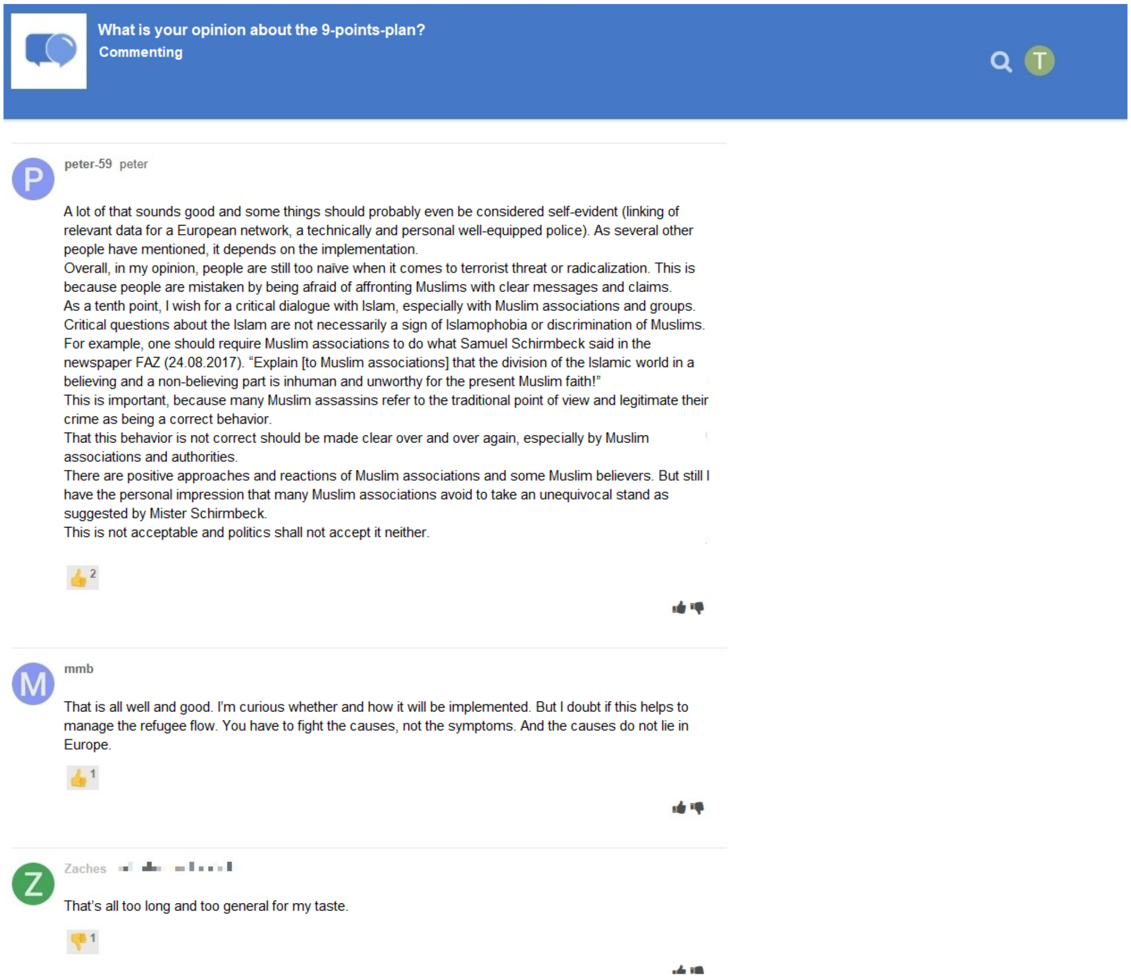

Figure 3. Communication that took place on the website with like and dislike buttons. (Translated to English.)

could be matched successfully. I excluded 29 participants who finished the questionnaire at T2 in less than three minutes, which were considered to be unreasonably fast.[2] To detect atypical data, I calculated Cook's distance. I excluded two participants who provided clear response patterns (i.e., straight-lining). The final sample included $N = 559$ participants. The sample characteristics at T1 and T2 were as follows: T1: age = 45 years, sex = 49% male, college degree = 22%. T2: age = 46 years, sex = 49% male, college degree = 29%.

[2] I preregistered to delete participants with less than 6 minutes answer time. However, this led to the exclusion of too many data points of high quality, which is why I relaxed this criterion. In the OSM, I report also the results using all participants.

One participant did not report their sex.

Measures

Wherever possible, I operationalized the variables using established measures. Where impossible (for example, to date there exists no scale on privacy deliberation), I self-designed novel items, which were pretested concerning legibility and understandability. To assess factor validity I ran confirmatory factor analyses (CFA). If the CFAs revealed insufficient fit, I deleted malfunctioning items. All items were formulated as statements to which participants indicated their (dis-)agreement on a bipolar 7-point scale. Answer options were visualized as follows: -3 (*strongly disagree*), -2 (*disagree*), -1 (*slightly disagree*), 0 (*neutral*), +1 (*slightly agree*), +2 (*agree*), +3 (*strongly agree*). For the analyses, answers were coded from 1 to 7. In the questionnaire, all items measuring a variable were presented on the same page in randomized order.

For an overview of the means, standard deviations, factorial validity, and reliability, see Table 1. For an overview of the variables' distributions, see Figure 4. For the exact wording of all items and their individual distributions, see OSM.

Privacy concerns. Privacy concerns were measured with seven items based on Buchanan, Paine, Joinson, and Reips (2007). One example item was "When using the participation platform, I had concerns about my privacy". One item was deleted due to poor psychometric properties.

Gratifications. I differentiated between two separate types of gratifications. *General gratifications* were measured with five items based on Sun, Wang, Shen, and Zhang (2015). One example item was "Using the participation platform has paid off for me". *Specific gratifications* were measured with 15 items on five different subdimensions with three items each. The scale was based on Scherer and Schlütz (2002). Example items were: "Using the participation platform made it possible for me to" … "learn things I would not have noticed otherwise" (information), "react to a subject that is important to me"

Table 1

Psychometric Properties, Factorial Validity, and Reliability of Measures

	m	sd	chisq	df	pvalue	cfi	tli	rmsea	srmr	omega	ave
Privacy concerns	3.21	1.51	11.04	9.00	0.27	1.00	1.00	0.02	0.01	0.96	0.80
General gratifications	4.76	1.22	34.03	5.00	0.00	0.98	0.95	0.10	0.02	0.93	0.74
Specific gratifications	4.71	1.02	269.77	85.00	0.00	0.94	0.93	0.06	0.05	0.95	0.59
Privacy deliberation	3.93	1.29	15.55	5.00	0.01	0.98	0.96	0.06	0.02	0.85	0.53
Self-efficacy	5.25	1.12	3.23	1.00	0.07	0.99	0.96	0.06	0.01	0.83	0.59
General trust	5.21	1.04	2.07	1.00	0.15	1.00	0.99	0.04	0.01	0.87	0.70
Specific trust	5.08	0.94	99.48	26.00	0.00	0.96	0.94	0.07	0.04	0.93	0.62

Note. omega = Raykov's composite reliability coefficient omega; avevar = average variance extracted.

(relevance), "engage politically" (political participation), "try to improve society" (idealism), and "soothe my guilty consciences" (extrinsic benefits).

Privacy deliberation. Privacy deliberation was measured with five self-designed items. One example item was "While using the participation platform I have weighed the advantages and disadvantages of writing a comment."

Self-efficacy. Self-efficacy was captured with six self-designed items, which measured whether participants felt that they had sufficient self-efficacy to write a comment on the website. For example, "I felt technically competent enough to write a comment." Two inverted items were deleted due to poor psychometric properties.

Trust. I differentiated between two types of trust. *General trust* was operationalized based on Söllner et al. (2016), addressing three targets (i.e., provider, website, and other users) with one item each. One example item was "The operators of the participation platform seemed trustworthy." *Specific trust* was operationalized for the same three targets with three subdimensions each (i.e., ability, benevolence/integrity, and

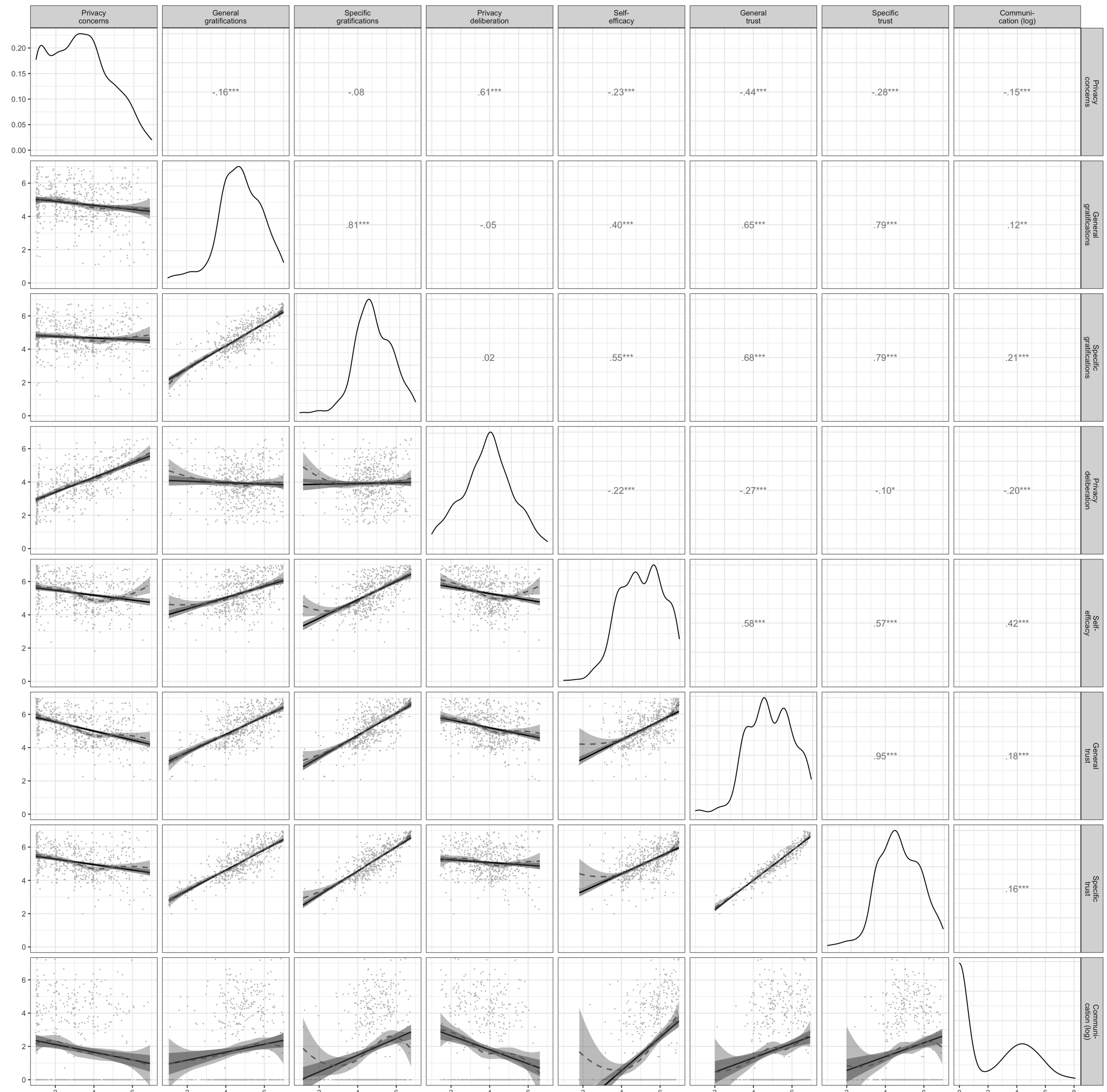

Figure 4. Above diagonal: zero-order correlation matrix; diagonal: density plots for each variable; below diagonal: bivariate scatter plots for zero-order correlations. Solid regression lines represent linear regressions, dotted regression lines represent quadratic regressions. Calculated with the model predicted values for each variable (baseline model).

reliability), which were measured with one item each. Example items were “The operators of the participation platform have done a good job” (ability), “The other users had good intentions” (benevolence/integrity), “The website worked well” (reliability). The results showed that the provider and website targets were not sufficiently distinct, as was evidenced by a Heywood case (i.e., standardized coefficient greater than 1). I hence adapted the scale to combine these two targets. The updated scale showed adequate fit.

Communication. Communication was calculated by counting the number of words each participant wrote in a comment. Communication was heavily skewed. Many people did communicate not at all, while some communicated a lot. Hence, the sum of words was log-scaled.

Data analysis

All hypotheses and research questions were tested using structural equation modeling with latent variables. The influence of the three websites was analyzed using contrast coding. I could therefore test the effects of experimental manipulations within a theoretical framework while using latent variables (Kline, 2016). Because the dependent variable communication was not normally distributed, I estimated the model using robust maximum likelihood (Kline, 2016). As recommended by Kline (2016), to assess global fit I report the model's χ^2, RMSEA (90% CI), CFI, and SRMR. Because sociodemographic variables are often related to communication and other privacy-related concepts (Tifferet, 2019), I controlled all variables for the influence of sex, age, and education. Preregistered hypotheses were tested with a one-sided significance level of 5%. Research questions were tested with a two-sided 5% significance level using family-wise Bonferroni-Holm correction. Exploratory analyses were conducted from a descriptive perspective. The reported p-values and confidence intervals should thus not be overinterpreted.

I used R (Version 4.2.2; R Core Team, 2018) and the R-packages *lavaan* (Version 0.6.13; Rosseel, 2012), *papaja* (Version 0.1.1; Aust & Barth, 2018), *pwr* (Version 1.3.0; Champely, 2018), *quanteda* (Version 3.2.4; Benoit, 2018), *semTools* (Version 0.5.6; Jorgensen et al., 2018), and *tidyverse* (Version 1.3.2; Wickham, 2017) for all analyses.

Results

Descriptive Analyses

I first measured and plotted all bivariate relations between the study variables (see Figure 4). No relationship was particularly curvilinear. Furthermore, all variables referring to the privacy calculus demonstrated the expected relationships with communication. For example, people who were more concerned about their privacy disclosed less information (r). Worth noting, specific gratifications predicted communication better than general gratifications (r vs. r). The mean of privacy deliberation was $m = 3.93$. Altogether, 32% of participants reported having actively deliberated about their privacy.

Note that the bivariate results showed three large correlations: specific trust and general gratifications ($r = .79$), privacy concerns and privacy deliberation ($r = .61$), and specific gratifications and self-efficacy ($r = .55$). As all six variables were later analyzed within a single multiple regression, problems of multicollinearity might occur.

Privacy Calculus

Preregistered analyses. First, I ran a model as specified in the preregistration. The model fit the data okay, $\chi^2(388) = 954.97$, $p < .001$, CFI = .94, RMSEA = .05, 90% CI [.05, .05], SRMR = .05. Regarding H1, I did not find that general gratifications predicted communication (β = -.04, b = -0.05, 95% CI [-0.21, 0.11], z = -0.64, p = .260; one-sided). With regard to H2, privacy concerns did not significantly predict communication (β = .04, b = 0.08, 95% CI [-0.25, 0.41], z = 0.47, p = .318; one-sided). RQ1 similarly revealed that privacy deliberation was not correlated with communication (β = -.10, b = -0.16, 95% CI [-0.34, 0.03], z = -1.68, p = .093; two-sided). Regarding H3, however, I found that experiencing self-efficacy predicted communication substantially (β = .39, b = 0.81, 95% CI [0.51, 1.10], z = 5.38, p < .001; one-sided). Concerning H4, results showed that trust was not associated with communication (β = -.10, b = -0.25, 95% CI [-0.80, 0.29], z = -0.92, p = .178; one-sided).

However, these results should be treated with caution. I found several signs of multicollinearity, such as large standard errors or “wrong” signs of predictors (Grewal, Cote, & Baumgartner, 2004). In the multiple regression trust had a *negative* relation with communication, whereas in the bivariate analysis it was *positive*.

Exploratory analyses. I slightly adapted the preregistered model on the basis of the insights described above. First, instead of specific trust and general gratifications I included *general* trust and *specific* gratifications, which were correlated slightly less strongly. The adapted model fit the data comparatively well, $\chi^2(507) = 1495.15$, $p < .001$, CFI = .93, RMSEA = .06, 90% CI [.06, .06], SRMR = .06.

In the adapted privacy calculus model, specific gratifications were positively related to communication online ($\beta = .14$, $b = 0.40$, 95% CI [> -0.01, 0.79], $z = 1.96$, $p = .050$; two-sided). People who deliberated more about their privacy disclosed less information ($\beta = -.13$, $b = -0.20$, 95% CI [-0.38, -0.01], $z = -2.09$, $p = .037$; two-sided). Self-efficacy remained substantially correlated with communication ($\beta = .35$, $b = 0.72$, 95% CI [0.44, 1.00], $z = 4.99$, $p < .001$; two-sided). Notably, I found a negative correlation between trust and communication ($\beta = -.16$, $b = -0.48$, 95% CI [-0.92, -0.05], $z = -2.16$, $p = .031$; two-sided), which again implies multicollinearity.

When confronted with multicollinearity, two responses are typically recommended (Grewal et al., 2004): (a) combining collinear variables into a single measure, or (b) keeping only one of the collinear variables. Combining variables was not an option in this case, because both trust and expected benefits are theoretically distinct constructs. And because *several* variables were closely related to one another, I therefore decided to fit a simple privacy calculus model containing only privacy concerns and specific gratifications.

The simple model fit the data well, $\chi^2(202) = 710.65$, $p < .001$, CFI = .95, RMSEA = .07, 90% CI [.06, .07], SRMR = .05. First, I found that people who experienced more privacy concerns than others disclosed less information ($\beta = -.13$, $b = -0.19$, 95% CI [-0.31, -0.07], $z = -3.14$, $p = .002$; two-sided). Second, people who reported more specific gratifications than others communicated more information ($\beta = .22$, $b = 0.63$, 95% CI [0.35, 0.92], $z = 4.37$, $p < .001$; two-sided). Both effect sizes were above the predefined SESOI of $r = .10$, which implies that the they were large enough to be theoretically relevant.

When comparing the three models with one another, the adapted model explained the most variance in communication (NA %), followed by the preregistered model (NA %), and the simple privacy calculus model (NA %). At the same time, the simple privacy calculus model was the most parsimonious one (BIC = 44,140, AIC = 43,500), followed by the preregistered model (BIC = 55,931, AIC = 55,040), and the adapted model (BIC = 64,411, AIC = 63,403). For a visual overview of all results, see Figure 5.

Popularity Cues

Preregistered analyses. In a next step, I analyzed the potential effects of the popularity cues. I for example expected that websites with like buttons would lead to more communication, gratifications, and privacy deliberation and to less privacy concerns. Somewhat surprisingly, I found no effects of the popularity cues on the privacy calculus variables. For an illustration, see Figure 6, which displays the model-predicted values for each variable (using the baseline model). The results show that the confidence intervals of all preregistered variables overlap, illustrating that there were no statistically significant differences across websites. For the detailed results of the specific inference tests using contrasts, see the OSM.

Exploratory analyses. The picture remained the same also when analyzing variables not included in the preregistration. Note that some differences missed statistical significance only marginally (e.g., specific gratifications for the comparison between the website with like buttons and the control website without like and dislike buttons). Nevertheless, I refrain from reading too much into these subtle differences. I conclude that the three websites were comparable regarding the privacy calculus variables and the amount of communication.

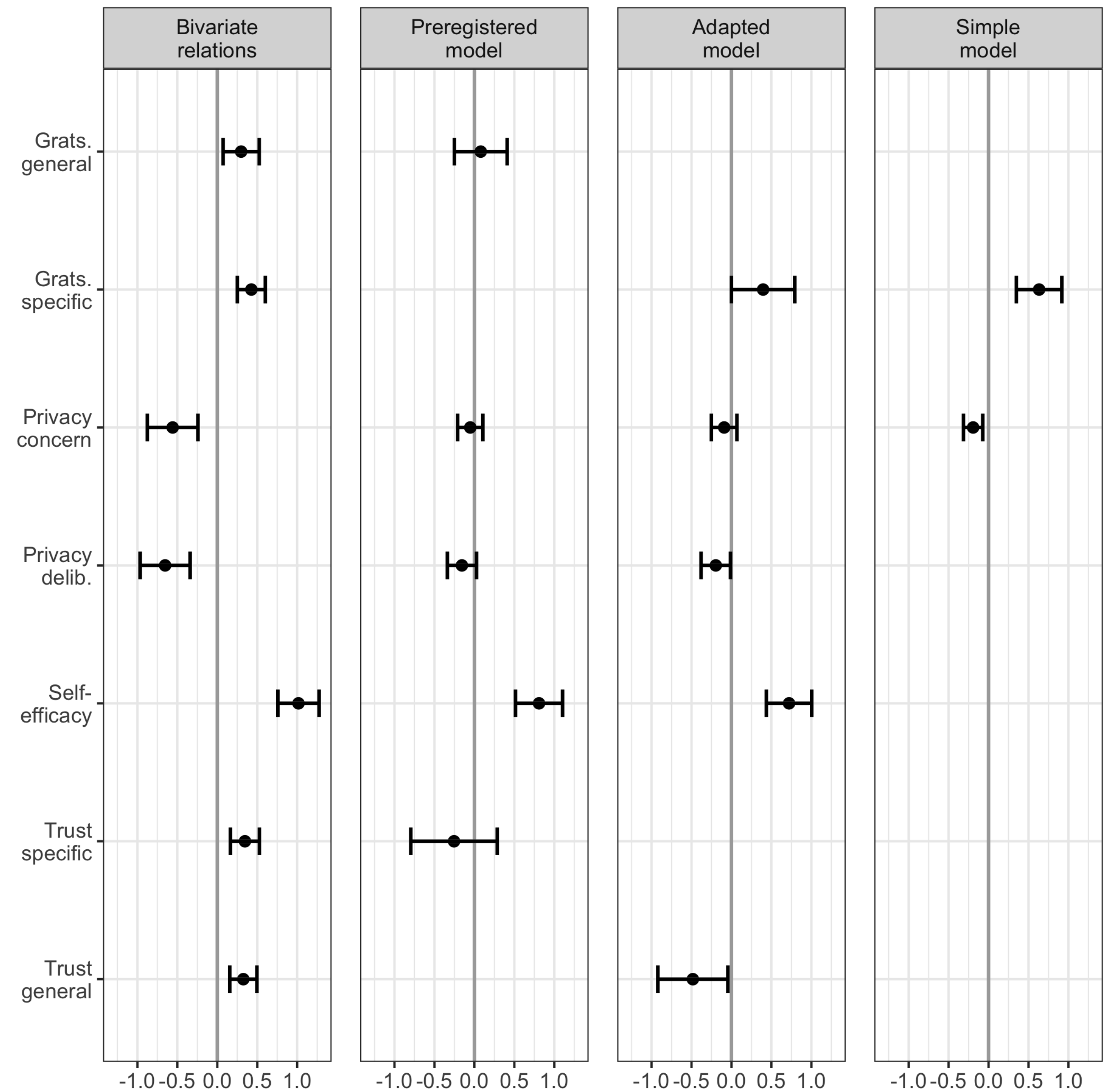

Figure 5. Predictors of communication. Displayed are the 95% CIs of unstandardized effects.

Discussion

This is the first study to analyze the privacy calculus using actual observed behavior in a preregistered field experiment. The data stem from a representative sample of the German population. I extended the theoretical privacy calculus model by explicitly testing privacy deliberation processes. I included self-efficacy and trust as additional variables, to

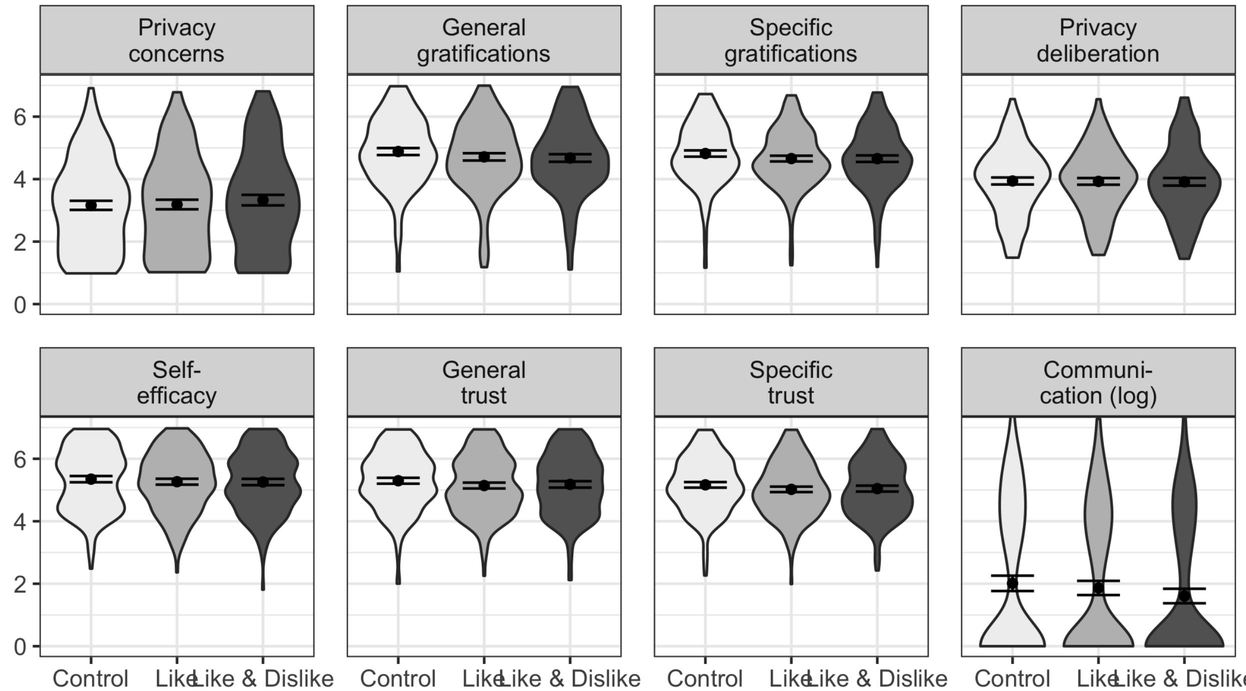

Figure 6. Overview of the model-predicted values for each variable, separated for the three websites. Control: Website without buttons. Like: Website with like buttons. Like & Dislike: Website with like and dislike buttons.

better represent the theoretical premise of bounded rationality. I further asked whether the privacy calculus is affected by popularity cues such as like and dislike buttons.

In the bivariate analyses, all privacy calculus variables significantly predicted communication activity. Thus, all variables likely play an important role when it comes to understanding online-communication. In the preregistered analyses using multiple regression, however, only self-efficacy significantly predicted communication. All other variables were not significant. There seems to be a relevant overlap between variables, and their mutual relation is still not clear. The preregistered extended privacy calculus model was therefore not supported by the data. However, the model showed problems typical of multicollinearity, which is why I also explored (a) an adapted version of the preregistered model, in which I exchanged two variables, and (b) a simple privacy calculus model, which included only privacy concerns and specific gratifications.

The adapted model suggests that also when holding all other variables constant, people who deliberate more about their privacy disclose less. People who expect more specific gratifications and who feel more self-efficacious disclose more. However, the model also suggests that if trust increases, while all other factors remain constant, communication decreases, which seems theoretically implausible. As a result, I also fit a simple privacy calculus model, which showed that both privacy concerns and obtained gratifications significantly and meaningfully predicted communication. Taken together, the results support the privacy calculus framework and suggest that in specific contexts communication online is not erratic and that it can be explained by several psychological variables. At the same time, variables such as trust and efficacy seem to play an important role, which further supports the underlying premise of bounded rationality.

The results suggest that in new communication contexts at least one third of all Internet users *actively deliberates* about their privacy. Determining whether this figure is large or small is difficult. Although the effect seems substantial to us, one could argue that it should be higher and that more people should actively deliberate about their online communication. Interestingly, results showed that privacy deliberation and privacy concerns were remarkably similar. Both variables were strongly correlated and showed comparable correlations with other variables. This either implies that thinking about privacy increases concerns or, conversely, that being concerned about privacy encourages us to ponder our options more carefully. Future research might tell.

Popularity cues do not always seem to have a strong influence on the privacy calculus and communication. Although some studies reported that popularity cues can substantially impact behavior (Muchnik et al., 2013), in this study I found the opposite. Users disclosed the same amount of personal information regardless of whether or not a website included like or dislike buttons. The results do not imply that popularity cues have no impact on the privacy calculus in general. Instead, they suggest that there exist certain contexts in which the influence of popularity cues is negligible.

The results also have methodological implications. First, one can question the tendency to further increase the complexity of the privacy calculus model by adding additional variables (e.g., Dienlin & Metzger, 2016). "Since all models are wrong the scientist cannot obtain a"correct" one by excessive elaboration. [...] Just as the ability to devise simple but evocative models is the signature of the great scientist so overelaboration and overparameterization is often the mark of mediocrity" (Box, 1976, p. 792). For example, it seems that adding self-efficacy to privacy calculus models is of limited theoretical value. Self-efficacy is often only a self-reported proxy of behavior and offers little incremental insight. Instead, it might be more interesting to find out *why* some people feel sufficiently efficacious to communicate whereas others do not.

In addition, although adding variables increases explained variance, it can also introduce multicollinearity. Multicollinearity is not a problem per se, but rather a helpful warning sign (Vanhove, 2019). From a *statistical* perspective, strongly correlated predictors mean that standard errors become larger (Vanhove, 2019). We can be less certain about the effects, because there is less unique variance (Vanhove, 2019). As a remedy, researchers could collect larger samples, which would increase statistical power and precision. Using accessible statistical software it is now possible to run a priori power analyses that explicitly account for correlated or collinear predictors (Wang & Rhemtulla, 2020).

From a *theoretical* perspective, multicollinearity could also suggest that the underlying theoretical model is ill-configured. It is my understanding that multiple regression is often used to isolate effects, to make sure that they are not caused by other third variables. However, in cases of highly correlated variables this often does not make much sense theoretically. Combining trust and gratification in a multiple regression asks how increasing benefits affects communication *while holding trust constant.* However, it seems more plausible to assume that increasing gratifications also automatically increases trust (Söllner et al., 2016). In the preregistered analysis I even went further and tested whether trust increases communication while holding constant gratifications, privacy concerns, privacy deliberations, and self-efficacy—an unlikely scenario. In short, the effects I found could be correct, but the interpretation is more difficult, potentially artificial, and thereby of little theoretical and practical value.

Finally, I found a surprisingly strong correlation between specific trust and expected gratifications (i.e., $r = .79$). Operationalizations of trust are remarkably close to expected gratifications. To illustrate, the trust subdimension *ability* includes items such as "The comments of other users were useful". Trust is often operationalized as a formative construct that directly results from factors such as expected benefits (Söllner et al., 2016). In conclusion, it is important not to confuse *causes* of trust with *measures* of trust. I thus recommend using general and reflective measures of trust.

Limitations

Although I did not find significant effects of like and dislike buttons in this study, they could still affect the privacy calculus in other contexts and settings. All findings are limited to the context I analyzed and should not be overly generalized. Null-findings pose the *Duhème-Quinn Problem* (Dienes, 2008). They can either result from an actual non-existence of effects or, instead, from a poor operationalization of the research question. In this case, it was not possible to send participants notifications when their comments were liked or disliked, which significantly decreased the popularity cues' salience.

The results do not allow for causal interpretation. First, all results are based on analyses of between-person variance. However, between-person relations often do not translate to within-person effects (Hamaker, Kuiper, & Grasman, 2015). Likewise, the mediation model is only suggestive, as I did not experimentally manipulate the mediating variables and also did not use a longitudinal design.

The self-reported measures were collected *after* the field phase in which the dependent variable was measured. As a result, the coefficients might overestimate the actual relations, because demand effects might have led participants to artificially align their theoretical answers with their practical behavior.

The assumption of stable unit treatment states that in experiments only the experimental variable should be manipulated, while all others should be held constant (Kline, 2016). In this study, I explicitly manipulated the popularity cues. However, because the experiment was conducted in the field several other variables could not be held constant, such as the content of communication by other users, the unfolding communication dynamics, and the characteristics of other users. As a result, the assumption of stable unit treatment was violated.

Conclusion

In this study I have found some support for the privacy calculus approach. People who were more concerned about their privacy disclosed less information online, whereas people who received more gratifications from using a website disclosed more information online. A substantial share of internet users, approximately 30%, engaged in a privacy calculus by actively deliberating about whether or not to disclose information. Popularity cues such as like and dislike buttons played only a minor role in this process. In conclusion, the results provide further evidence against the privacy paradox. Internet users are at least somewhat proactive and reasonable—maybe no more or less proactive or reasonable than in other everyday situations.

References

Acquisti, A., Brandimarte, L., & Loewenstein, G. (2020). Secrets and Likes: The Drive for Privacy and the Difficulty of Achieving It in the Digital Age. *Journal of Consumer Psychology*, *30*(4), 736–758. https://doi.org/https://doi.org/10.1002/jcpy.1191

Altman, I. (1976). Privacy: A conceptual analysis. *Environment and Behavior*, *8*(1), 7–29. https://doi.org/10.1177/001391657600800102

Aust, F., & Barth, M. (2018). *papaja: Create APA manuscripts with R Markdown.* Retrieved from https://github.com/crsh/papaja

Barnes, S. B. (2006). A privacy paradox: Social networking in the United States. *First Monday*, *11*(9). Retrieved from www.firstmonday.org/issues/issue11_9/barnes/index.html

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

Bendor, J. (2015). Bounded Rationality. In *International Encyclopedia of the Social & Behavioral Sciences* (pp. 773–776). Elsevier. https://doi.org/10.1016/B978-0-08-097086-8.93012-5

Benoit, K. (2018). *Quanteda: Quantitative analysis of textual data.* https://doi.org/10.5281/zenodo.1004683

Bol, N., Dienlin, T., Kruikemeier, S., Sax, M., Boerman, S. C., Strycharz, J., … Vreese, C. H. (2018). Understanding the effects of personalization as a privacy calculus: Analyzing self-disclosure across health, news, and commerce contexts. *Journal of Computer-Mediated Communication*, *23*(6), 370–388. https://doi.org/10.1093/jcmc/zmy020

Box, G. E. P. (1976). Science and statistics. *Journal of the American Statistical Association*, *71*(356), 791–799. https://doi.org/10.1080/01621459.1976.10480949

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*(2), 157–165. https://doi.org/10.1002/asi.20459

Carr, C. T., Hayes, R. A., & Sumner, E. M. (2018). Predicting a threshold of perceived Facebook post success via likes and reactions: A test of explanatory mechanisms. *Communication Research Reports*, *35*(2), 141–151. https://doi.org/10.1080/08824096.2017.1409618

Champely, S. (2018). *Pwr: Basic functions for power analysis*. Retrieved from https://CRAN.R-project.org/package=pwr

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

Cohen, J. (1992). A power primer. *Psychological Bulletin*, *112*(1), 155–159. https://doi.org/10.1037/0033-2909.112.1.155

Dhir, A., & Tsai, C.-C. (2017). Understanding the relationship between intensity and gratifications of Facebook use among adolescents and young adults. *Telematics and Informatics*, *34*(4), 350–364. https://doi.org/10.1016/j.tele.2016.08.017

Dienes, Z. (2008). *Understanding psychology as a science: An introduction to scientific and statistical inference*. New York, N.Y.: Palgrave Macmillan.

Dienlin, T. (2014). The privacy process model. In S. Garnett, S. Halft, M. Herz, & J. M. Mönig (Eds.), *Medien und Privatheit* (pp. 105–122). Passau, Germany: Karl Stutz.

Dienlin, T. (2017). *The psychology of privacy: Analyzing processes of media use and interpersonal communication*. Hohenheim, Germany: University of Hohenheim.

Retrieved from http://opus.uni-hohenheim.de/volltexte/2017/1315/

Dienlin, T., Masur, P. K., & Trepte, S. (2021). A longitudinal analysis of the privacy paradox. *New Media & Society*, 14614448211016316. https://doi.org/10.1177/14614448211016316

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

Ellison, N. B., & Vitak, J. (2015). Social network site affordances and their relationship to social capital processes. In S. S. Sundar (Ed.), *The handbook of the psychology of communication technology* (pp. 205–227). Chichester, MA: Wiley Blackwell.

Ellison, N. B., Vitak, J., Steinfield, C., Gray, R., & Lampe, C. (2011). Negotiating privacy concerns and social capital needs in a social media environment. In S. Trepte & L. Reinecke (Eds.), *Privacy online: Perspectives on privacy and self-disclosure in the social web* (pp. 19–32). Berlin, Germany: Springer. https://doi.org/10.1007/978-3-642-21521-6_3

Evans, S. K., Pearce, K. E., Vitak, J., & Treem, J. W. (2017). Explicating affordances: A conceptual framework for understanding affordances in communication research. *Journal of Computer-Mediated Communication*, *22*(1), 35–52. https://doi.org/10.1111/jcc4.12180

Fox, J., & McEwan, B. (2017). Distinguishing technologies for social interaction: The perceived social affordances of communication channels scale. *Communication Monographs*, *9*, 1–21. https://doi.org/10.1080/03637751.2017.1332418

Gefen, D., Karahanna, E., & Straub, D. W. (2003). Trust and TAM in online shopping: An integrated model. *MIS Q*, *27*(1), 5190. Retrieved from http://dl.acm.org/citation.cfm?id=2017181.2017185

Gibson, J. J. (2015). *The ecological approach to visual perception*. New York, NY: Psychology Press.

Gigerenzer, G., Selten, R., & Workshop, D. (Eds.). (2002). *Bounded rationality: The adaptive toolbox* (1. MIT Press paperback ed). Cambridge, Mass.: MIT Press. Retrieved from https://external.dandelon.com/download/attachments/dandelon/ids/DE0041B967843B1BDDEE6C12578B1001CB0D1.pdf

Grewal, R., Cote, J. A., & Baumgartner, H. (2004). Multicollinearity and measurement error in structural equation models: Implications for theory testing. *Marketing Science*, *23*(4), 519–529. https://doi.org/10.1287/mksc.1040.0070

Hamaker, E. L., Kuiper, R. M., & Grasman, R. P. P. P. (2015). A critique of the cross-lagged panel model. *Psychological Methods*, *20*(1), 102–116. https://doi.org/10.1037/a0038889

Heirman, W., Walrave, M., & Ponnet, K. (2013). Predicting adolescents' disclosure of personal information in exchange for commercial incentives: An application of an extended theory of planned behavior. *Cyberpsychology, Behavior, and Social Networking*, *16*(2), 81–87. https://doi.org/10.1089/cyber.2012.0041

Jorgensen, D., T., Pornprasertmanit, S., Schoemann, M., A., … Y. (2018). *semTools: Useful tools for structural equation modeling*. Retrieved from https://CRAN.R-project.org/package=semTools

Kahneman, D. (2011). *Thinking, fast and slow*. New York: Farrar, Straus; Giroux.

Kline, R. B. (2016). *Principles and practice of structural equation modeling* (4th ed.). New York, NY: The Guilford Press.

Knijnenburg, B., Raybourn, E., Cherry, D., Wilkinson, D., Sivakumar, S., & Sloan, H. (2017). Death to the privacy calculus? *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.2923806

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

Koohikamali, M., French, A. M., & Kim, D. J. (2019). An investigation of a dynamic model of privacy trade-off in use of mobile social network applications: A longitudinal perspective. *Decision Support Systems*, *119*, 46–59. https://doi.org/10.1016/j.dss.2019.02.007

Krämer, N. C., & Schäwel, J. (2020). Mastering the challenge of balancing self-disclosure and privacy in social media. *Current Opinion in Psychology*, *31*, 67–71. https://doi.org/10.1016/j.copsyc.2019.08.003

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

Lakens, D., Scheel, A. M., & Isager, P. M. (2018). Equivalence testing for psychological research: A tutorial. *Advances in Methods and Practices in Psychological Science*, *1*(2), 259–269. https://doi.org/10.1177/2515245918770963

Laufer, R. S., & Wolfe, M. (1977). Privacy as a concept and a social issue: A multidimensional developmental theory. *Journal of Social Issues*, *33*(3), 22–42. https://doi.org/10.1111/j.1540-4560.1977.tb01880.x

Li, Y. (2011). Empirical studies on online information privacy concerns: Literature review and an integrative framework. *Communications of the Association for Information Systems*, *28*, 453–496.

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

Min, J., & Kim, B. (2015). How are people enticed to disclose personal information despite privacy concerns in social network sites? The calculus between benefit and cost. *Journal of the Association for Information Science and Technology, 66*(4), 839–857. https://doi.org/10.1002/asi.23206

Muchnik, L., Aral, S., & Taylor, S. J. (2013). Social influence bias: A randomized experiment. *Science (New York, N.Y.), 341*(6146), 647–651. https://doi.org/10.1126/science.1240466

New York Public Radio. (2018). *The privacy paradox* [{InternetDocument}]. Retrieved from https://project.wnyc.org/privacy-paradox/

Omarzu, J. (2000). A disclosure decision model: Determining how and when individuals will self-disclose. *Personality and Social Psychology Review, 4*(2), 174–185. https://doi.org/10.1207/S15327957PSPR0402_5

Petty, R., & Cacioppo, J. (1986). *Communication and Persuasion: Central and Peripheral Routes to Attitude Change*. New York: Springer-Verlag. https://doi.org/10.1007/978-1-4612-4964-1

R Core Team. (2018). *R: A language and environment for statistical computing.* Vienna, Austria: R Foundation for Statistical Computing. Retrieved from https://www.R-project.org/

Reinecke, L., & Trepte, S. (2014). Authenticity and well-being on social network sites: A two-wave longitudinal study on the effects of online authenticity and the positivity bias in SNS communication. *Computers in Human Behavior, 30*, 95–102. https://doi.org/10.1016/j.chb.2013.07.030

Rosoff, H., Cui, J., & John, R. S. (2013). Heuristics and biases in cyber security dilemmas. *Environment Systems and Decisions, 33*(4), 517–529. https://doi.org/10.1007/s10669-013-9473-2

Rosseel, Y. (2012). lavaan: An R package for structural equation modeling. *Journal of Statistical Software, 48*(2), 1–36. Retrieved from http://www.jstatsoft.org/v48/i02/

Scherer, H., & Schlütz, D. (2002). Gratifikation à la minute: Die zeitnahe Erfassung von Gratifikationen. In P. Rössler (Ed.), *Empirische Perspektiven der Rezeptionsforschung* (pp. 133–151). Munich, Germany: Reinhard Fischer.

Simon, H. A. (1990). Bounded Rationality. In J. Eatwell, M. Milgate, & P. Newman (Eds.), *Utility and Probability* (pp. 15–18). London: Palgrave Macmillan UK. https://doi.org/10.1007/978-1-349-20568-4_5

Söllner, M., Hoffmann, A., & Leimeister, J. M. (2016). Why different trust relationships matter for information systems users. *European Journal of Information Systems*, *25*(3), 274–287. https://doi.org/10.1057/ejis.2015.17

Solove, D. (2020). The Myth of the Privacy Paradox. *GW Law Faculty Publications & Other Works*. Retrieved from https://scholarship.law.gwu.edu/faculty_publications/1482

Stroud, N. J., Muddiman, A., & Scacco, J. M. (2017). Like, recommend, or respect?: Altering political behavior in news comment sections. *New Media & Society*, *19*(11), 1727–1743. https://doi.org/10.1177/1461444816642420

Sumner, E. M., Ruge-Jones, L., & Alcorn, D. (2017). A functional approach to the Facebook Like button: An exploration of meaning, interpersonal functionality, and potential alternative response buttons. *New Media & Society*, *20*(4), 1451–1469. https://doi.org/10.1177/1461444817697917

Sun, Y., Wang, N., Shen, X.-L., & Zhang, J. X. (2015). Location information disclosure in location-based social network services: Privacy calculus, benefit structure, and gender differences. *Computers in Human Behavior*, *52*, 278–292. https://doi.org/10.1016/j.chb.2015.06.006

Taddicken, M., & Jers, C. (2011). The uses of privacy online: Trading a loss of privacy for social web gratifications? In S. Trepte & L. Reinecke (Eds.), *Privacy online: Perspectives on privacy and self-disclosure in the social web* (pp. 143–158). Berlin, Germany: Springer.

Tifferet, S. (2019). Gender differences in privacy tendencies on social network sites:

A meta-analysis. *Computers in Human Behavior*, *93*, 1–12. https://doi.org/10.1016/j.chb.2018.11.046

Trepte, S., Scharkow, M., & Dienlin, T. (2020). The privacy calculus contextualized: The influence of affordances. *Computers in Human Behavior*, *104*, 106115. https://doi.org/10.1016/j.chb.2019.08.022

Vanhove, J. (2019). *Collinearity isn't a disease that needs curing.* Retrieved from https://osf.io/8x4uc/

Wang, Y. A., & Rhemtulla, M. (2020). *Power analysis for parameter estimation in structural equation modeling: A discussion and tutorial.* https://doi.org/10.31234/osf.io/pj67b

Whiting, A., & Williams, D. (2013). Why people use social media: A uses and gratifications approach. *Qualitative Market Research: An International Journal*, *16*(4), 362–369. https://doi.org/10.1108/QMR-06-2013-0041

Wickham, H. (2017). *Tidyverse: Easily install and load the 'tidyverse'.* Retrieved from https://CRAN.R-project.org/package=tidyverse