Likes or Dislikes, Gratifications or Concerns? A One-Week Field Experiment Analyzing the Effects of Popularity Cues on the Privacy Calculus in Online Communication

Abstract

The privacy calculus model states that people weigh risks and benefits before communicating online. This paper analyzes three questions: How robust is the privacy calculus, can it be replicated with actual behavior in realistic online settings? Do we need to extend the model by integrating more socio-psychological measures such as trust, self-efficacy, and privacy deliberation? How strongly is the privacy calculus affected by affordances such as like and dislike buttons? In a preregistered one-week field experiment (N = 590), participants discussed a current political topic on an online website, which included either (a) like buttons, (b) both like and dislike buttons, or (c) no buttons. The privacy calculus model was confirmed: Benefits and concerns affected communication. Deliberating about privacy by comparing benefits and risks decreased communication, whereas experiencing self-efficacy and trust increased communication. Although like and dislike buttons did not affect concerns, experiences, trust, efficacy, and deliberation, they had a strong effect on behavior: They reduced communication by 45 percent.

Keywords: privacy calculus, communication, popularity cues, field experiment, preregistration

Word count: 8,204

Likes or Dislikes, Gratifications or Concerns? A One-Week Field Experiment Analyzing the Effects of Popularity Cues on the Privacy Calculus in Online Communication

Introduction

According to the privacy paradox, the way users share information online is erratic (Barnes, 2006): Although being strongly concerned about their privacy, people communicate much personal information online (Taddicken & Jers, 2011). However, despite its popularity in both academic research (Masur, 2023) and the public press (New York Public Radio, 2018), empirical support for the privacy paradox is tenuous (Baruh et al., 2017). Research is increasingly building on the privacy calculus model (Dienlin, 2023), which states that communication online can be explained by perceived risks and expected benefits (Bol et al., 2018; Krasnova et al., 2010).

Although the privacy calculus has gained momentum in academic research, several important questions remain unanswered. First, the privacy calculus' empirical foundation needs to be improved (Knijnenburg et al., 2017). To date, much research on the privacy calculus builds on (a) self-reports of behavior (Krasnova et al., 2010), (b) vignette approaches (Bol et al., 2018), or (c) one-shot experiments in the lab (Trepte et al., 2020). Self-reports are often unreliable measures of online behavior (Parry et al., 2021), vignette approaches have limited external validity, and one-shot experiments cannot analyze effects of sustained use. The first aim is therefore to replicate the privacy calculus model in a more authentic and long-term setting using actual behavioral data. Doing so will show its robustness, and it will help understand if behavior is better explained by the privacy paradox approach or by the privacy calculus model.

Second, the privacy calculus model is criticized for neglecting the actual process of weighing pros and cons, and for over-emphasizing rationality (Knijnenburg et al., 2017). According to critics, simply showing that both concerns and gratifications correlate with communication online does not prove that an explicit weighing process took place. Instead,

we would need to find out if people deliberately compare costs and benefits before communicating online. Therefore, I will also analyze the process of comparing pros and cons explicitly, by elaborating on what I will call the the privacy deliberation process (Omarzu, 2000). Next, focusing exclusively on costs and benefits might not fully capture how and why users engage online. I, hence, extend the privacy calculus by analyzing how online communication is affected by trust and self-efficacy, two variables less focused on rationality and more oriented toward socio-psychological aspects critical in online contexts (Metzger, 2004).

Online behavior is determined by the person itself and their external circumstances (Bazarova & Masur, 2020; Spottswood & Hancock, 2017; Trepte et al., 2020). The privacy calculus upholds that much of behavior is rational and self-determined, but how strongly does this process depend on online affordances? It is well known that the affordances of many online services are optimized to elicit as much interaction as possible (Ellison & Vitak, 2015; Masur et al., 2021), for example via low threshold communication features such as likes, shares, replies, or reactions (Carr et al., 2018). Implicit and explicit cues on how a website is used can increase communication (Spottswood & Hancock, 2017; Trepte et al., 2020). How large are the effects of external popularity cues such as like and dislike buttons compared to the internal weighing of pros and cons? And how easily can the mechanisms of the privacy calculus be affected by means of popularity cues?

In conclusion, in this paper we contribute to communication theory by means of (a) replication, (b) falsification, (c) extending the range of existing theory, (d) elucidating mechanisms, and (e) theory comparison (DeAndrea & Holbert, 2017).

Replicating the Privacy Calculus

The privacy calculus analyzes why people communicate online. When are we willing to engage in a conversation? It builds on the calculus of behavior (Laufer & Wolfe, 1977) and states that people are weighing risks and benefits before actively communicating. Communication is closely related to privacy, which is defined as a “voluntary and

temporary withdrawal of a person from the general society" (Westin, 1967, p. 7). People regulate their privacy by deciding what and what not to communicate (Dienlin, 2014). Communication is therefore also closely related to self-disclosure. Just as it is impossible to not communicate, communication inherently promotes self-disclosure. In a recent study, communication quantity and the frequency of expressing one's political opinion was almost indistinguishable ($r = .91$; AUTHORS). Next to breadth and depth, communication quantity is hence often considered a central dimension of self-disclosure (Omarzu, 2000).

Sharing information carries risks, as recipients may reuse it in different contexts, potentially harming the original sender (Masur et al., 2021). As a result, people who aim to avoid risks should be inclined to share less information, especially in online contexts where audiences are much larger (Vitak, 2012). Indeed, empirical research confirms that people with higher privacy needs and privacy concerns are less likely to communicate online (Krasnova et al., 2010; Masur, 2023; Masur & Trepte, 2021). This finding is now confirmed by several meta-analyses and reviews (Baruh et al., 2017; Dienlin & Sun, 2021; Gerber et al., 2018). Similarly, people who are more concerned about their privacy also engage in more privacy protection behaviors (Baruh et al., 2017; Stubenvoll et al., 2022).

Even outweighing concerns, the most relevant drivers of online communication are expected gratifications (Bol et al., 2018; Dienlin & Metzger, 2016; Kezer et al., 2022). On average, people are happy to trade in parts of their privacy to receive something more valuable in return (Laufer & Wolfe, 1977). In online communication, the most important benefits include social support, social capital, entertainment, information-seeking, and self-presentation (Dhir & Tsai, 2017; Ellison et al., 2007; Krasnova et al., 2010; Whiting & Williams, 2013).

H1: People who are more concerned about their privacy 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.

Extending the Privacy Calculus

Although privacy calculus implies that people explicitly compare benefits and risks before communicating online, prior research has neglected this aspect (Knijnenburg et al., 2017). Only observing that privacy concerns or expected gratifications and communication online are related does not prove that an explicit weighing process took place (Knijnenburg et al., 2017). Instead, we need to analyze if, and if so by how much, people actively deliberate about their privacy by comparing benefits and risks, and whether doing so influences their willingness to communicate. Self-disclosure theory (Altman, 1976; Omarzu, 2000) suggests that if the benefits of communication are attractive, deciding whether or not to communicate is a "conscious and deliberative process" (Omarzu, 2000, p. 183). I hence introduce and investigate a novel concept termed *privacy deliberation*. Privacy deliberation captures the extent to which individuals explicitly compare risks and benefits before communicating with others.

How could deliberating about one's privacy affect communication? On the one hand, it could reduce subsequent communication. Refraining from communication—the primary means of connecting with others (Altman, 1976)—often requires restraint (Omarzu, 2000). This is especially true for social media, which are designed to foster communication and participation (Ellison & Vitak, 2015; Masur et al., 2021). Actively thinking about whether communicating is worthwhile might be the first step not to participate. In addition, actively reflecting about one's behavior represents a central and Type 2 approach toward decision making, which is often associated with more critical and cautious behavior (Kahneman, 2011; Petty & Cacioppo, 1986).

On the other hand, deliberating about privacy might also increase communication. The default behavior in online contexts is passively browsing the content, but not actively engaging in communication (Ozimek et al., 2023). Especially in new contexts without prior experience, actively pondering one's options might trigger users to leave their default state of passiveness and to become active and involved. In light of the numerous benefits

mentioned above, it might make sense to conclude that participation is beneficial, thereby fostering communication (Krasnova et al., 2010).

RQ1: Do people who deliberate more actively about their privacy communicate more or less online?

It is useful to understand the privacy calculus from the perspective of *bounded rationality* (Simon, 1990). Bounded rationality states that "(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). It is important to emphasize that although human behavior is considered *partly* irrational, bounded rationality does not state that it is *completely* irrational (Gigerenzer et al., 2002). Instead, rationality needs to be understood as a continuum. And in the context of online privacy, rationality is impeded by information asymmetries, presence bias, intangibility, illusory control, or herding (Acquisti et al., 2020). It follows that to provide a more complete picture, additional factors less focused on rationality but more on socio-psychological aspects should also explain communication.

Two central factors that help us understand online communication are self-efficacy and trust (Hossain & Wigand, 2004; Metzger, 2004). Privacy violations create psychological distress (Ledbetter, 2019). Experiencing online contexts as a safe space that users can sufficiently control is important for engaging in online communication. If users are more familiar, experienced, and knowledgeable in a given online context, they are more likely to navigate that online contexts successfully and to communicate actively (Baruh et al., 2017; Krämer & Schäwel, 2020; Park, 2013). People with more privacy self-efficacy engage more successfully in self-withdrawal (Dienlin & Metzger, 2016) and protective online behavior (Boerman et al., 2021; van Ooijen et al., 2022). Hence, if users possess more self-efficacy to participate, they should also communicate more.

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

In all situations where people lack experience, control, or competence, a central variable to understand behavior is trust (Gefen et al., 2003). Trust plays a key role especially in online contexts (Metzger, 2004, 2006). Users often cannot control the environment or the way their information is handled (Acquisti et al., 2020; Bräunlich et al., 2020). Trust either captures "*specific* beliefs dealing primarily with the integrity, benevolence, and ability of another party" (Gefen et al., 2003, p. 55, emphasis added) or a "*general* belief that another party can be trusted" (Gefen et al., 2003, p. 55, emphasis added). In online contexts, there are different targets of trust, including (a) the information system, (b) the provider, (c) the Internet, and (d) the community of other users (Söllner et al., 2016). People who put more trust in the providers of networks, for example, disclose more personal information (Li, 2011). To comprehensively capture and understand online communication, trust should hence be included.

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

Analyzing the Impact of Popularity Cues

How are the privacy calculus and communication affected by the context, the digital infrastructure? How easily can the calculus be manipulated externally? One of the central tools to afford and govern online behavior are popularity cues such as like and dislike buttons (Stsiampkouskaya et al., 2023). Popularity cues have been shown to affect behavior (Krämer & Schäwel, 2020; Masur et al., 2021; Trepte et al., 2020). For example, online comments that already have several dislikes are more likely to receive further dislikes (Muchnik et al., 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 et al., 2017).

How and why might popularity cues affect the privacy calculus? In analyzing this question, it makes sense to analyze the cues' underlying affordances (Ellison & Vitak, 2015; Fox & McEwan, 2017). Affordances are mental representations of how objects might be used. They emphasize that it is not the *objective features* that determine behavior, but

rather our *subjective perceptions* (Gibson, 2015). Popularity cues such as like and dislike buttons, which are of primary interest in this study, are understood as "paralinguistic digital affordances" (Carr et al., 2018, p. 142), lowering thresholds to partake in online communication.

Popularity cues likely impact the privacy calculus via two underlying theoretical mechanisms (Krämer & Schäwel, 2020): First, the *mere presence* of popularity cues might affect whether people are willing to disclose. Being able to attract likes might afford active communication. The mere option to receive dislikes, conversely, might inhibit communication. Second, *actually receiving* likes or dislikes might affect behavior, by means of positive reinforcement (likes) or punishment (dislikes) (Skinner, 2014). To illustrate, likes are affirmative and embody the positivity bias of social media (Schreurs et al., 2022). Receiving a like online is similar to receiving a compliment offline (Carr et al., 2018; Sumner et al., 2017). Like buttons afford and emphasize a *gain frame* (Rosoff et al., 2013). These gains can be garnered only through active participation. In situations where people can gain immediate positive outcomes, concerns and risks that are more vague and in the future often become less relevant (presence bias, Ainslie & Haslam, 1992). Because like buttons emphasize positive outcomes, it is likely that concerns decrease. In situations where there is more to win, people might also more actively deliberate about whether or not to communicate.

Dislikes, instead, represent a punishment, introducing a *loss frame*. Websites featuring both like *and* dislike buttons should therefore be more ambivalent compared to websites without popularity cues, fostering privacy deliberation. Privacy concerns should not be reduced anymore: People who need more privacy are also more shy and risk averse (Dienlin & Metzger, 2024). Implementing the dislike button might therefore increase privacy concerns, canceling out the positive effects of the like button. At the same time, communication and benefits might still be increased compared to a website without like and dislikes buttons, as online benefits are often considered to outweigh risks (positivity

bias, Schreurs et al., 2022).

H5. Compared to a control group with no like and 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 a control group with no like and 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.

In conclusion, this leads to an updated and extended model of the privacy calculus, in which the affordances of online contexts affect communication mediated via experienced privacy concerns, expected gratifications, privacy deliberation, self-efficacy, and trust. For an overview of the theoretical model, see Figure 1.

Methods

Open Science

This manuscript features a companion website, which includes the data, research materials, analysis scripts, and a reproducible version of this manuscript (see https://XMtRa.github.io/like_dislike). The hypotheses, sample size, research materials, analyses, and exclusion criteria were preregistered (see https://osf.io/a6tzc/?view_only=5d0ef9fe5e1745878cd1b19273cdf859). In some cases, the preregistered approach had to be changed (see companion website). Analyses not preregistered are reported as exploratory analyses.

Procedure

The study was designed as an online field experiment with three different groups. The first experimental group used a website that included like buttons; the second

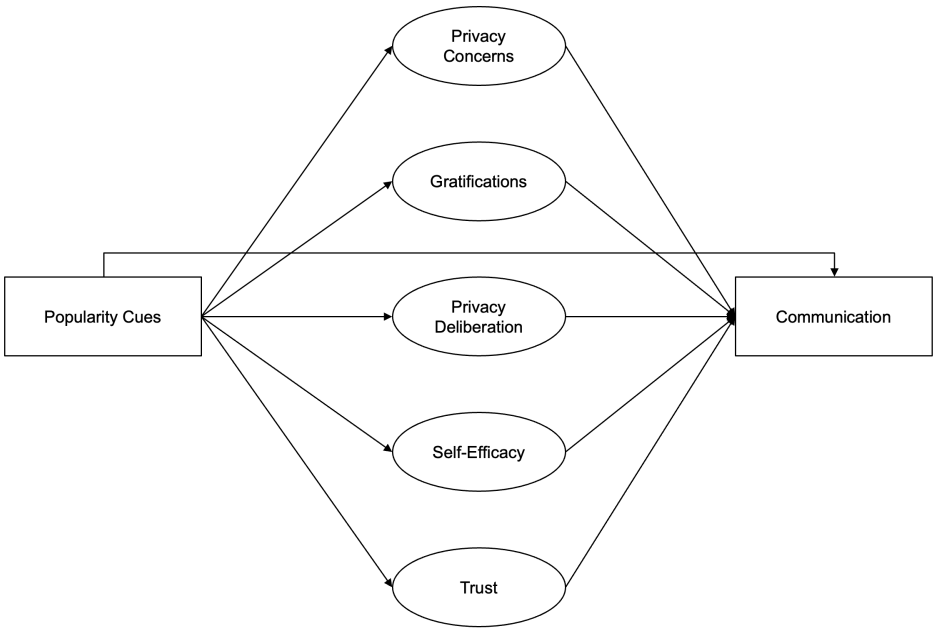

Figure 1

Overview of the extended privacy calculus model.

experimental group used an identical website including both like and dislike buttons; and the control group used an identical website without like and dislike buttons. Participants were randomly distributed to one of the three websites in a between-subject design.

The data were collected in Germany. Participants were recruited using the professional panel agency Norstat. As incentive, participants were awarded digital points, to receive special offers from online retailers. Participants had to be over 18 years old and reside in Germany. In a first step, the company sent its panel members an invitation to participate in the study. In this invitation, panel members were asked to participate in a study analyzing the current threat posed by terrorist attacks. Members who agreed to participate were sent the first questionnaire (*T1*). The questionnaire asked participants about their sociodemographic background, (b) provided more details about the study, and (c) included a registration link for the website, which was introduced 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 visit the website and to discuss the topic of the terrorism threat in Germany. Participants could use the website and write comments over the course of one week. Subsequently, participants received a follow-up questionnaire in which the self-reported measures reported below were collected (*T2*).

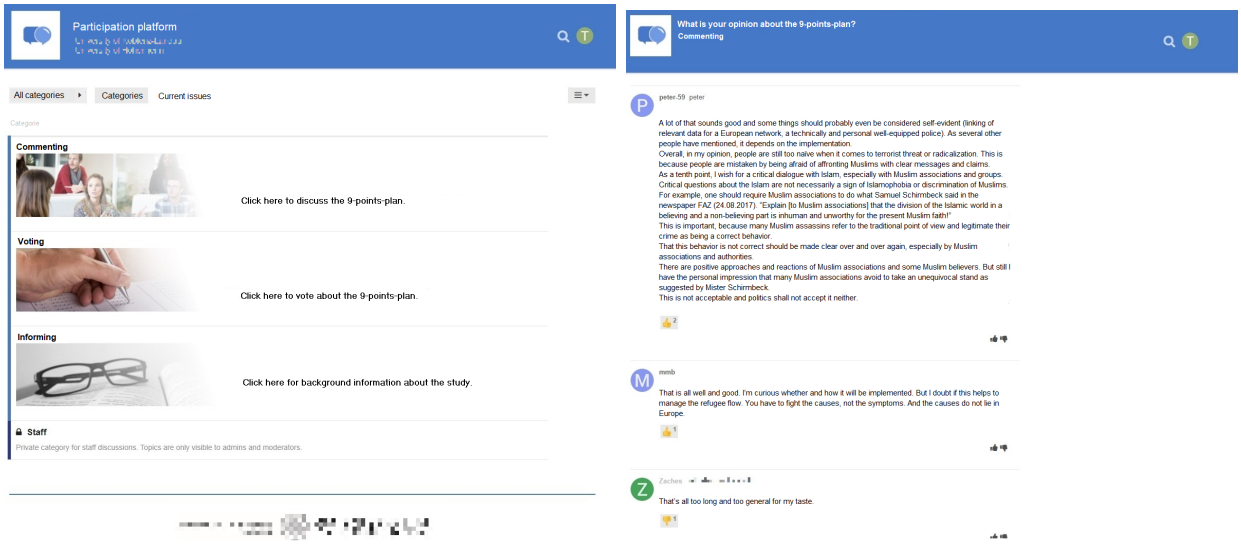

Figure 2

Screenshot of the landing page and of communication taking place. Translated into English.

The online website was programmed based on the open-source software *discourse* (https://www.discourse.org/). To make sure the website was professional and authentic, several pretests with students from the local university were run. 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. All communication was checked, and there were no instances of people providing meaningless text or doubting the experiment. For a screenshot of the landing page and for examples of comments, see Figure 2.

Participants

Sample size was determined using a priori power analyses. The power analyses were based on estimates from the literature. When researching aspects of privacy online (e.g., Baruh et al., 2017), effects are often small (i.e., $r = .10$, Cohen, 1992). Hence, the minimum effect size was set to be $r = .10$. The aim was to be able to detect this effect with a probability of at least 95% (i.e., power = 95%). Using the regular alpha level of 5%, power analyses suggested a minimum sample size of $N = 1{,}077$. In the end, I was able to include $N = 559$ in the analyses (see below), which was significantly lower than the original aim. With this sample size, the study had a power of 77% to find an effect at least as large as $r = .10$. Sensitivity analyses showed that the current study could still make reliable results (i.e., with a power of 95%) for effects at least as large as $r = .14$. In conclusion, although not as powerful as planned, the study is still adequately powered to find the small effects reported in the privacy literature (Baruh et al., 2017).

A quota sample that matched the German population in terms of age, gender, 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. The data were connected using tokens and IP addresses. For technical reasons, the data of several participants could not be matched (for example, because they used different devices for the respective steps). In the end, the data of 590 participants could be matched successfully. Considered unreasonably fast, twenty-nine participants were excluded who finished the questionnaire at T2 in less than three minutes. To detect atypical data and response patterns, Cook's distance was calculated. I excluded two participants with 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, gender = 49% male, college degree = 22%. T2: age = 46 years, gender = 49% male, college degree = 29%. One participant did not report their gender.

Table 1

Psychometric Properties, Factorial Validity, and Reliability of Measures

	m	sd	chisq	df	p-value	cfi	tli	rmsea	srmr	omega	ave
Privacy concerns	3.21	1.51	11.04	9	0.27	1.00	1.00	0.02	0.01	0.96	0.80
Gratifications	4.76	1.22	34.03	5	0.00	0.98	0.95	0.10	0.02	0.93	0.74
Privacy deliberation	3.93	1.29	15.55	5	0.01	0.98	0.96	0.06	0.02	0.85	0.53
Self-efficacy	5.21	1.04	3.23	1	0.07	0.99	0.96	0.06	0.01	0.83	0.59
Trust general	5.08	0.94	2.07	1	0.15	1.00	0.99	0.04	0.01	0.87	0.70
Trust specific	5.25	1.12	89.11	24	0.00	0.96	0.94	0.07	0.04	0.93	0.61

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

Measures

Factor validity was assessed using confirmatory factor analyses (CFA). If the CFAs revealed insufficient fit, malfunctioning items were deleted. All items were measured on bipolar 7-point scales. 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. All items measuring the same variable were presented in randomized order on the same page.

All measures showed high factorial validity. For an overview of the means, standard deviations, factorial validity, and reliability, see Table 1. For the variables' distributions, see Figure 3. For all items and their distributions, see companion website.

Privacy concerns were measured with seven items based on Buchanan et al. (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. The mean was $m = 3.21$. This value is below the scale's midpoint of 4, showing that on average people were not strongly concerned about their privacy.

General gratifications were measured with five items based on Sun et al. (2015). One example item was "Using the participation platform has paid off for me". The mean was $m = 4.76$, which was above the scale's midpoint. This shows that on average people considered the website to be beneficial. For exploratory analyses, we also collected a scale measuring specific gratifications, not included here.

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." The mean lay on the scale's neutral midpoint ($m = 3.93$). (For an interpretation, see below.)

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. People felt self-efficacious to use the website ($m = 5.21$).

Two types of trust were measured. *General trust* was operationalized based on Söllner et al. (2016), addressing three targets (i.e., provider, website, and other users), measured 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 sub-dimensions each (i.e., ability, benevolence/integrity, and reliability), 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). Participants placed a lot of trust in the website, the providers and the other users (trust general: $m = 5.08$; trust specific: $m = 5.25$).

Communication was calculated by counting the number of words each participant wrote in a comment. Communication was zero-inflated and heavily skewed: While 58 percent did not communicate at all, the maximum number of words communicated by a

single user was 3198 words. On average, participants wrote 77 words.

Data Analysis

As preregistered, all hypotheses and research questions were initially tested using structural equation modeling with latent variables. The influence of the three websites was analyzed using contrast coding. Because the assumption of multivariate normality was violated, I estimated the models 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. To exclude confounding influences, I controlled all variables for age, gender, and education, which have been shown to affect both privacy concerns and online communication (Masur, 2023; Tifferet, 2019). The preregistered hypotheses were tested with a one-sided significance level of 5%; the research questions were tested with a two-sided 5% significance level using family-wise Bonferroni-Holm correction.

As became apparent when analyzing the data, the preregistered analyses had two major problems. First, communication was zero-inflated and gamma distributed. Although it is possible to analyze non-normal data with structural equation modeling, it is recommended to use analyses that model the variables' distribution, which can be achieved with Bayesian hurdle models (McElreath, 2016). In conclusion, in the exploratory analyses I ran (unstandardized) Bayesian hurdle regression models, modeling the outcome as a zero-inflated gamma distribution using default (flat) priors (chains = 4, iterations = 2,000, warm-up = 1,000, Bürkner, 2017). Second, in the preregistered analyses several variables were combined that are theoretically and empirically closely related, leading to multicollinearity (Vanhove, 2021). As a remedy, I adopted a causal modeling perspective, controlling only for confounders—in this case, age, gender, and education—but not for mediators (Rohrer, 2018). To assess the effects, I tested whether or not the 95% highest density intervals of the average marginal effects excluded zero. If they excluded zero, effects can be considered "significant" (McElreath, 2016). I also plotted the distribution of the effects. For more information on the fitted models, see online companion website.

The data were analyzed using R (Version 4.4.0; R Core Team, 2018) and the R-packages *brms* (Version 2.21.0; Bürkner, 2017, 2018), *lavaan* (Version 0.6.18; Rosseel, 2012), *marginaleffects* (Arel-Bundock, 2023), *papaja* (Version 0.1.2; Aust & Barth, 2018), *pwr* (Version 1.3.0; Champely, 2018), *quanteda* (Benoit, 2018), *semTools* (Version 0.5.6; Jorgensen et al., 2018), and *tidyverse* (Version 2.0.0; Wickham, 2017).

Results

Descriptive Analyses

I first plotted the bivariate relations of all variables (see Figure 3). All variables referring to the privacy calculus demonstrated the expected bivariate relationships with communication. For example, people who were more concerned about their privacy disclosed less information (r = -.15). The mean of privacy deliberation was m = 3.93. Altogether, 32% of participants reported having actively deliberated about their privacy.

The bivariate results showed two large correlations: specific trust and gratifications (r = .79), and privacy concerns and privacy deliberation (r = .61). As all six variables were later analyzed within a single multiple regression, problems of multicollinearity might occur.

Preregistered Analyses

First, as preregistered I ran a structural equation model with multiple predictors. The model fit the data okay, $\chi^2(387) = 934.98$, $p < .001$, cfi = .94, rmsea = .05, 90% CI [.05, .05], srmr = .05. With regard to H1, privacy concerns did not significantly predict communication ($\beta >$ -.01, b = -0.01, 95% CI [-0.30, 0.28], z = -0.07, p = .473; one-sided). Regarding H2, results showed that gratifications did not predict communication (β = -.02, b = -0.04, 95% CI [-0.19, 0.12], z = -0.45, p = .327; one-sided). RQ1 similarly revealed that privacy deliberation did not predict communication (β = -.10, b = -0.16, 95% CI [-0.35, 0.02], z = -1.76, p = .078; two-sided). Regarding H3, however, I found that experiencing self-efficacy predicted communication substantially (β = .37, b = 0.77, 95% CI [0.49, 1.05], z = 5.42, $p < .001$; one-sided). Concerning H4, results showed that trust was not

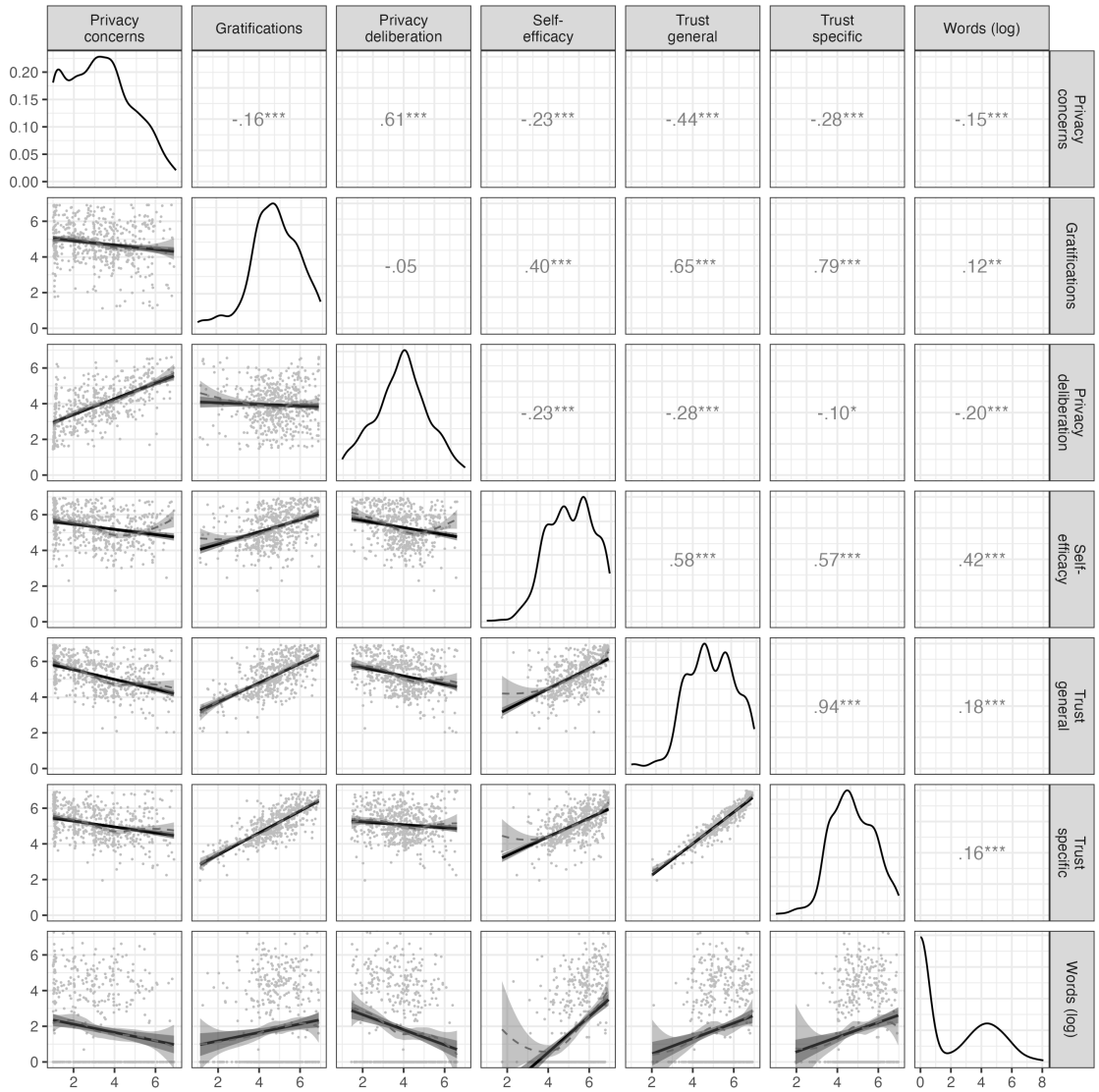

Figure 3

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).

associated with communication (β = -.03, b = -0.09, 95% CI [-0.56, 0.38], z = -0.36, p = .358; one-sided).

However, these results should be treated with caution. I found several signs of multicollinearity, evidenced by the large standard errors or "wrong" and reversed signs of

predictors (Vanhove, 2021). For example, in the bivariate analysis trust had a positive relation with communication, whereas in the multiple regression the effect was negative—which should make us skeptical.

Next, I analyzed the effects of the popularity cues. It was for example expected that websites with like buttons would lead to more communication, more gratifications, more privacy deliberation, and less privacy concerns. The results showed that the popularity cues had no effects on communication and on the privacy calculus variables.

For an illustration, see Figure 4. For the detailed results of the specific inference tests using contrasts, see companion website.

Exploratory Analyses

As explained above, the preregistered results were problematic. Communication was not normally distributed and the predictors were collinear. I hence updated the analyses, using Bayesian hurdle models controlling only for confounders but not mediators. In predicting communication, I opted for general trust over specific trust, as it exhibited lower levels of empirical and theoretical overlap with gratifications. The updated exploratory analyses showed different results.

Hypotheses 1, 2, 3, and 4 were all confirmed: If participants were more concerned about their privacy, they communicated less: With each one-point increase in privacy concerns, on average they wrote 16 words less (95% HDI: -28, -5). If participants expected more gratifications from participation, they communicated more actively: If their expected gratifications increased by one point, on average they also wrote 27 words more (95% HDI: 13, 44). If participants felt more self-efficacious, they communicated much more: If their self-efficacy increased by one point, on average they wrote 73 words more (95% HDI: 56, 94). The relationship was curvilinear, almost exponential: Whereas a change in self-efficacy from 1 to 2 only led to an "increase" of zero words, a change from 6 to 7 led to an increase of 103 words. Next, if participants experienced more trust in the website, provider, and other users, they also communicated much more: If their trust increased by one point, on

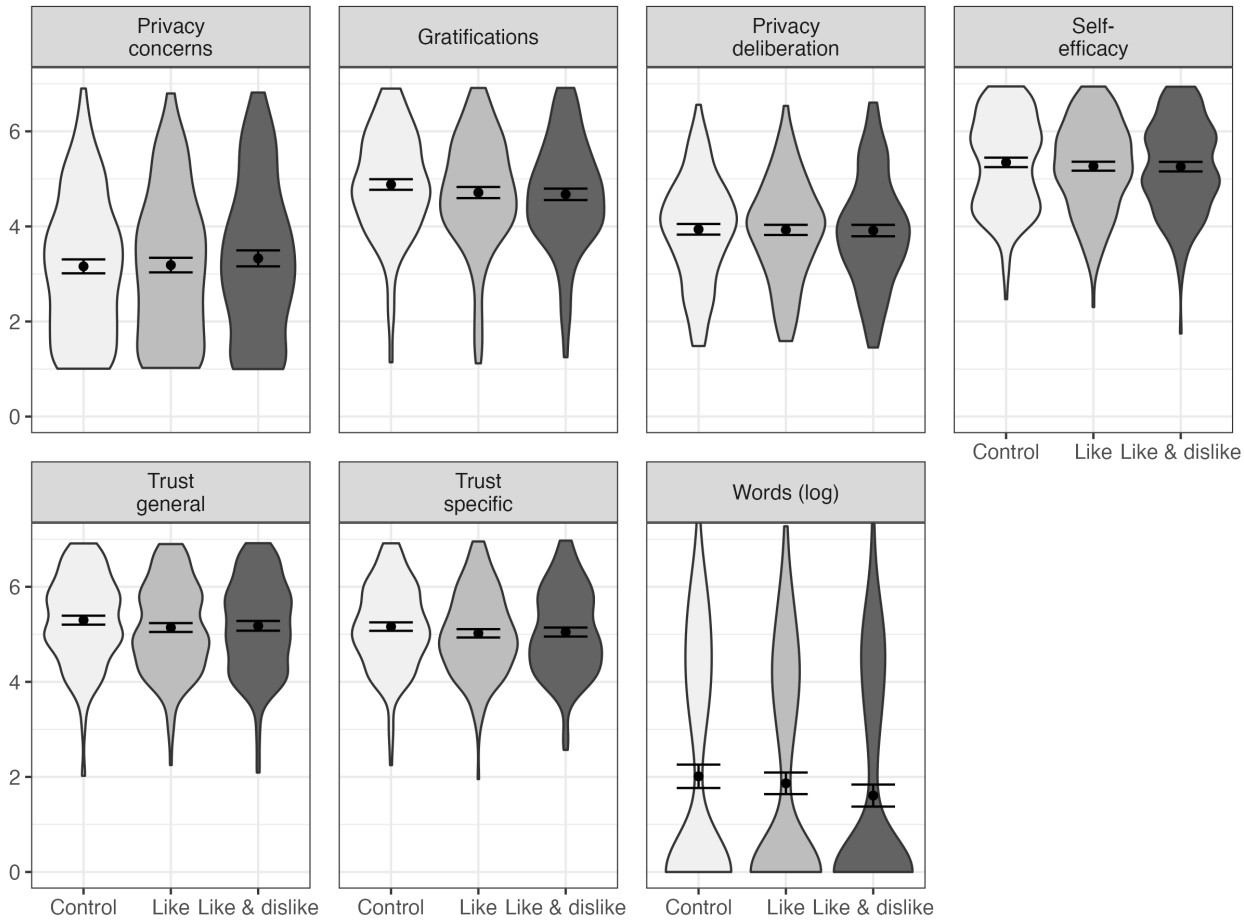

Figure 4

Distributions and means with 95% CIs 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. Values from preregistered SEM.

average they wrote 31 words more (95% HDI: 14, 54). The first research question asked how privacy deliberation would affect communication. The results revealed a negative effect. The more people deliberated about their privacy, the less they communicated. If privacy deliberation increased by one point, on average they wrote 33 words less (95% HDI: -51, -20).

I then reanalyzed the effects of the popularity cues on communication. Compared to

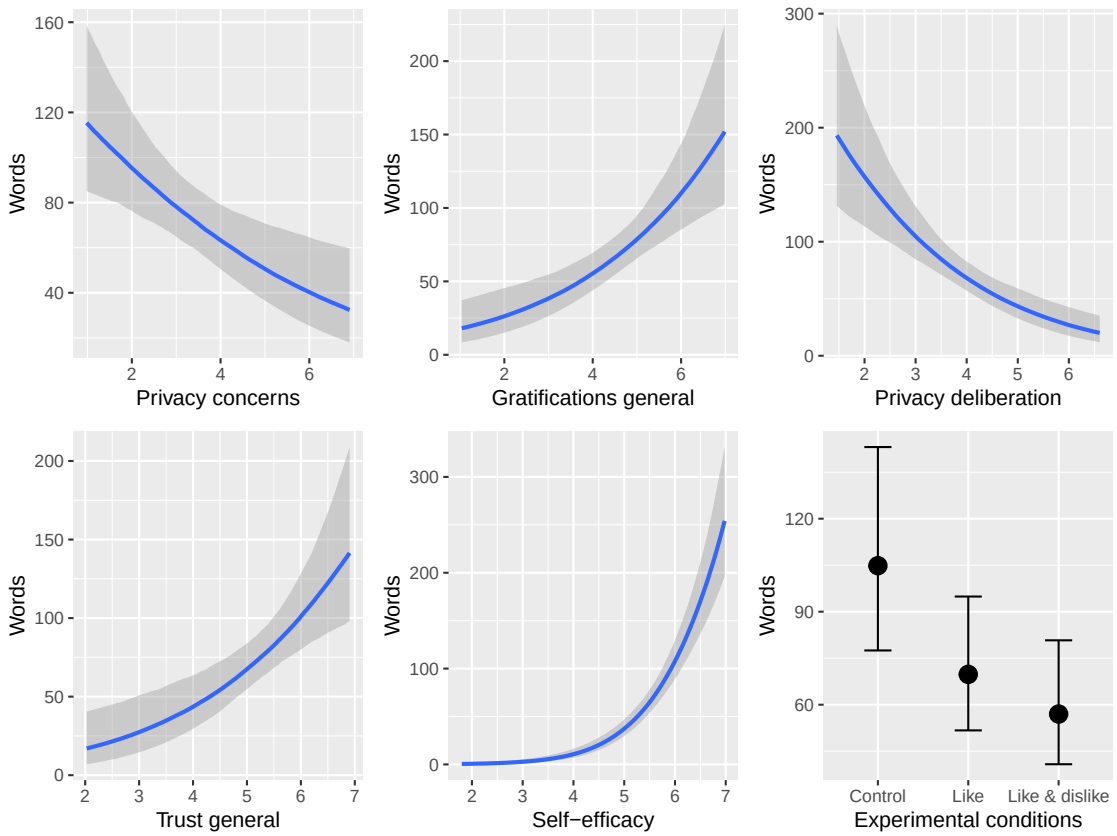

Figure 5

Exploratory analyses. Plotted are the average marginal effects of the Bayesian hurdle models. The difference between the control and the like & disklike group is significant.

the control condition without popularity cues, implementing like buttons did not significantly affect communication, b = -35 (95% HDI: -82, 4). But note that the effect was very close to not including the zero. However, implementing both like and dislike buttons affected communication. Contrary to what I expected, implementing both popularity cues *decreased* communication. If both popularity cues were present, participants on average wrote 48 words less (95% HDI: -93, -10). The introduction of both cues hence led to a 45% decline in number of words that were written.

Finally, I tested if the effect of the popularity cues on communication were potentially mediated by the privacy calculus variables. Results showed that this was not the case. The popularity cues only affected behavior but not the predictors of the privacy

Table 2

Unstandardized average marginal effects of the privacy calculus variables and the popularity cues on communication. Credibility intervals excluding zero are considered significant.

		95% HDI	
Predictor	Estimate	LL	UL
Privacy calculus			
Privacy concerns	-16	-28	-5
Expected gratifications	27	13	44
Privacy deliberation	-33	-51	-20
Trust	31	14	54
Self-efficacy	73	56	94
Experimental conditions			
Like & dislike vs. control	-48	-93	-10
Like vs. control	-35	-82	4
Like vs. like & dislike	13	-19	44

Note. HDI = highest density interval, LL = lower level; UL = upper level. Reported are average marginal effects.

calculus model (see online companion website). The results suggest that the effect was either direct or mediated by other variables not included here (Coenen, 2022).

Discussion

This study analyzed three questions: Can the privacy calculus can be replicated with behavioral data in an authentic setting? Should the privacy calculus model be extended theoretically? Do like and dislike buttons affect online communication and the privacy calculus? To this end, a preregistered field experiment was conducted, which lasted one week. The privacy calculus model was extended: The privacy deliberation processes was tested explicitly, and trust and self-efficacy were included as predictors.

The preregistered analyses showed that the popularity cues did not affect communication. Only self-efficacy emerged as a significant predictor of online communication. All other variables remained insignificant. However, the preregistered analyses have to be treated with caution. The predictors were collinear, which makes their integration in one single model problematic (Vanhove, 2021). In addition, the main variable and outcome of the study, number of communicated words, was zero-inflated and gamma distributed, which requires a different type of analysis. The preregistered analyses using structural equation modeling with multiple predictors were hence problematic.

To address these issues, I conducted Bayesian hurdle-gamma models (see section Data analysis). This updated approach changed the results. People who were more concerned about their privacy wrote fewer words. To illustrate, people who reported being very much concerned posted only 32 words on average, whereas people who reported being not concerned posted 115 words. People who experienced privacy concerns hence differed strongly in their communication behavior from people who were unconcerned. Participants who received more gratifications wrote substantially more words. The effect was even larger, almost twice as large. For each point-increase in gratifications, participants wrote 27 words more. Attaining benefits online is hence a strong predictor of online communication. Together, the results provide further support for the privacy calculus and against the privacy paradox (Baruh et al., 2017). Communication online does not seem to be overly illogical. To large extents, it is aligned with respondents' concerns and benefits.

Results showed that trust and self-efficacy were important drivers of online communication. Participants who placed more trust into the website, the providers, and the other community members communicated more actively. Interestingly, self-efficacy was the strongest of all predictors. Participants who felt more self-efficacious disclosed much more than others. To illustrate, if people reported no self-efficacy, they wrote only 1 word on average. However, when they reported high levels of self-efficacy, they wrote 254 words. This finding further supports the underlying premise of bounded rationality (Simon, 1990).

Although more rational aspects such as costs and benefits influence behavior, behavior is also determined by more socio-psychological variables such as trust and self-efficacy. The findings are therefore closely aligned with existing theory. For example, the technology acceptance model states that online behavior is most strongly determined by usefulness and ease of use (Venkatesh et al., 2003)—two variables closely related to gratifications and self-efficacy.

The privacy calculus was criticized for not explicitly analyzing the process of weighing pros and cons before disclosing (Knijnenburg et al., 2017). In this study, I thus elaborated on the privacy deliberation process. The results showed that only one third of all participants agreed to have actively weighed the benefits and risks before communicating on the platform. This figure seems comparatively low. Even in new online contexts, the majority of users does not actively deliberate about their online communication, suggesting that online use is to large extents implicit (Acquisti et al., 2020).

Interestingly, and perhaps also somewhat surprisingly, privacy deliberation and privacy concerns were strongly correlated ($r = .61$). If we are concerned we also think and deliberate more actively about our privacy. And if we are not concerned we do not deliberate. This finding can be aligned with decision theory (Elsbach & Barr, 1999): When being concerned, we are in a negative state; and when in a negative state, we judge more critically. At this point, it is still unknown if thinking about privacy increases concerns or, conversely, if growing more concerned about privacy makes us deliberate more carefully.

The updated results showed that implementing both like and dislike buttons decreased communication. This was an unexpected and interesting finding. It suggests that negative feedback, or perhaps even only risks of negative feedback, can stifle communication. The effect was strong: Implementing both like and dislikes cues led to a 45% decrease in number of written words. When compared to the privacy calculus variables, we see that the effect is of similar size: Growing a bit more concerned or receiving less gratifications have a comparable impact on behavior. This finding is aligned

with studies reporting strong effects of popularity cues on behavior (Muchnik et al., 2013).

The negative effects of dislike buttons might help explain why almost all existing successful social network sites have chosen to omit negative popularity cues. At the time of writing, only a handful of websites have (partially) implemented dislike buttons (e.g., youtube, stackexchange, or reddit). Despite the positivity bias of social media (Schreurs et al., 2022), chances of receiving negative feedback and communication are real, as can be seen by moral outrages or "shit-storms". Explicit negative popularity cues are low threshold paralinguistic affordances (Carr et al., 2018). They likely prime or trigger negative experiences or expectations, thereby stifling communication. Interestingly, however, they did not affect the privacy calculus variables, and no indirect effect was found. Hence, the effect is either transmitted via variables not included here (Coenen, 2022), or perhaps subconscious and direct.

Websites only including like buttons had no effect on the number of communicated words. If anything, there was an unexpected (non-significant) trend toward reduced communication. Although one might expect that like buttons, being positive feedback cues, increase communication, it is also plausible that they can decrease communication. Not receiving any likes can be perceived as ostracizing (Schneider et al., 2017). In the context of this study, participants discussed a political topic. Here, not receiving likes might be even more threatening and intimidating than on regular social media, where it is more common to discuss every-day and low-threshold topics. Although like buttons are commonplace in social media, the findings suggest that in specific contexts they inhibit communication.

Limitations

The main implications and results discussed above rest on exploratory analyses not registered a priori. Exploratory analyses are part of the research process, compatible with preregistration, and important for scientific progress. The updated analyses represent and document a learning process, which arguably led to an improved analysis. However, the results should still be considered somewhat preliminary, to be confirmed in subsequent

studies.

Whereas the effects of the popularity cues on all variables can be interpreted from a causal perspective (but see below), more caution is needed regarding the effects of the privacy calculus variables on communication. Although the effects were controlled for age, gender, and education, other variables not included here could potentially bias the causal estimates (Coenen, 2022). In addition, in order not to reveal the study intention the self-reported measures were collected after the field phase. Demand effects might have led participants to align their answers to their prior behavior. To illustrate, users who communicated more actively might have experienced more self-efficacy afterward. As a result, the coefficients might overestimate the actual effects.

In experiments only the treatment variable should be manipulated, while all others should be held constant (assumption of stable unit treatment, Kline, 2016). Being a field experiment, several 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. Future research should repeat the design, preferably using several runs of the same experiment, to further assess generalizability and robustness.

Conclusion

This study provides further support for the privacy calculus model and against the privacy paradox approach. Expected benefits, privacy concerns, deliberating about benefits and risks, trust, and self-efficacy all affected communication. Like and dislike buttons reduced communication significantly. Users can be considered proactive and reasonable. But, similar to everyday offline contexts, they are also affected by the affordances of their environment, and often act implicitly without pondering the consequences of their actions.

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/10.1002/jcpy.1191

Ainslie, G., & Haslam, N. (1992). Hyperbolic discounting. In *Choice over time* (pp. 57–92). Russell Sage Foundation.

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

Arel-Bundock, V. (2023). *Marginaleffects: Predictions, comparisons, slopes, marginal means, and hypothesis tests*. https://CRAN.R-project.org/package=marginaleffects

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

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

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

Bazarova, N. N., & Masur, P. K. (2020). Towards an integration of individualistic, networked, and institutional approaches to online disclosure and privacy in a networked ecology. *Current Opinion in Psychology*, *36*, 118–123. https://doi.org/10.1016/j.copsyc.2020.05.004

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

Boerman, S. C., Kruikemeier, S., & Zuiderveen Borgesius, F. J. (2021). Exploring

motivations for online privacy protection behavior: Insights from panel data. *Communication Research*, *48*(7), 953–977. https://doi.org/10.1177/0093650218800915

Bol, N., Dienlin, T., Kruikemeier, S., Sax, M., Boerman, S. C., Strycharz, J., Helberger, N., & 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

Bräunlich, K., Dienlin, T., Eichenhofer, J., Helm, P., Trepte, S., Grimm, R., Seubert, S., & Gusy, C. (2020). Linking loose ends: An interdisciplinary privacy and communication model. *New Media & Society*, 1461444820905045. https://doi.org/10.1177/1461444820905045

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

Bürkner, P.-C. (2017). brms: An R package for Bayesian multilevel models using Stan. *Journal of Statistical Software*, *80*(1), 1–28. https://doi.org/10.18637/jss.v080.i01

Bürkner, P.-C. (2018). Advanced Bayesian multilevel modeling with the R package brms. *The R Journal*, *10*(1), 395–411. https://doi.org/10.32614/RJ-2018-017

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.* https://CRAN.R-project.org/package=pwr

Coenen, L. (2022). The indirect effect is omitted variable bias. A cautionary note on the theoretical interpretation of products-of-coefficients in mediation analyses. *European*

Journal of Communication, 026732312210822. https://doi.org/10.1177/02673231221082244

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

DeAndrea, D. C., & Holbert, R. L. (2017). Increasing clarity where it is needed most: Articulating and evaluating theoretical contributions. *Annals of the International Communication Association*, *41*(2), 168–180. https://doi.org/10.1080/23808985.2017.1304163

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

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

Dienlin, T. (2023). Privacy calculus: Theories, studies, and new perspectives. In S. Trepte & P. Masur (Eds.), *The Routledge handbook of privacy and social media* (pp. 70–79). Routledge.

Dienlin, T., & Metzger, M. (2024). Who Needs Privacy? Exploring the Relations Between Need for Privacy and Personality. *Collabra: Psychology*, *10*(1), 120402. https://doi.org/10.1525/collabra.120402

Dienlin, T., & Metzger, M. J. (2016). An extended privacy calculus model for SNSs—Analyzing self-disclosure and self-withdrawal in a representative U.S. sample. *Journal of Computer-Mediated Communication*, *21*(5), 368–383. https://doi.org/10.1111/jcc4.12163

Dienlin, T., & Sun, Y. (2021). Does the privacy paradox exist? Comment on Yu et al.'s (2020) meta-analysis. *Meta-Psychology*, *5*. https://doi.org/10.15626/MP.2020.2711

Ellison, N. B., Steinfield, C., & Lampe, C. (2007). The benefits of Facebook "friends:" Social capital and college students' use of online social network sites. *Journal of*

Computer-Mediated Communication, *12*(4), 1143–1168. https://doi.org/10.1111/j.1083-6101.2007.00367.x

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* (Vol. v.33, pp. 205–227). Wiley Blackwell.

Elsbach, K. D., & Barr, P. S. (1999). The effects of mood on individuals' use of structured decision protocols. *Organization Science*, *10*(2), 181–198. https://doi.org/10.1287/orsc.10.2.181

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.

Gerber, N., Gerber, P., & Volkamer, M. (2018). Explaining the privacy paradox: A systematic review of literature investigating privacy attitude and behavior. *Computers & Security*, *77*, 226–261. https://doi.org/10.1016/j.cose.2018.04.002

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

Gigerenzer, G., Selten, R., & Workshop, D. (Eds.). (2002). *Bounded rationality: The adaptive toolbox* (1st ed.). MIT Press.

Hossain, L., & Wigand, R. T. (2004). ICT enabled virtual collaboration through trust. *Journal of Computer-Mediated Communication*, *10*(1), JCMC1014. https://doi.org/10.1111/j.1083-6101.2004.tb00233.x

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

Kahneman, D. (2011). *Thinking, fast and slow*. Farrar, Straus and Giroux.

Kezer, M., Dienlin, T., & Baruh, L. (2022). Getting the privacy calculus right: Analyzing

the relations between privacy concerns, expected benefits, and self-disclosure using response surface analysis. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace*, *16*(4). https://doi.org/10.5817/CP2022-4-1

Kline, R. B. (2016). *Principles and practice of structural equation modeling* (4th ed.). 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

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

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

Ledbetter, A. M. (2019). Parent-child privacy boundary conflict patterns during the first year of college: Mediating family communication patterns, predicting psychosocial distress. *Human Communication Research*, *45*(3), 255–285. https://doi.org/10.1093/hcr/hqy018

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.

Masur, P. K. (2023). Understanding the effects of conceptual and analytical choices on "finding" the privacy paradox: A specification curve analysis of large-scale survey data. *Information, Communication & Society*, *26*(3), 584–602.

https://doi.org/10.1080/1369118X.2021.1963460

Masur, P. K., DiFranzo, D., & Bazarova, N. N. (2021). Behavioral contagion on social media: Effects of social norms, design interventions, and critical media literacy on self-disclosure. *Plos One*, *16*(7), e0254670.

Masur, P. K., & Trepte, S. (2021). Transformative or not? How privacy violation experiences influence online privacy concerns and online information disclosure. *Human Communication Research*, *47*(1), 49–74. https://doi.org/10.1093/hcr/hqaa012

McElreath, R. (2016). *Statistical rethinking: A Bayesian course with examples in R and Stan*. CRC Press/Taylor & Francis Group.

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

Metzger, M. J. (2006). Effects of site, vendor, and consumer characteristics on web site trust and disclosure. *Communication Research*, *33*(3), 155–179. https://doi.org/10.1177/0093650206287076

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

New York Public Radio. (2018). *The privacy paradox*. 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

Ozimek, P., Brailovskaia, J., & Bierhoff, H.-W. (2023). Active and passive behavior in social media: Validating the Social Media Activity Questionnaire (SMAQ). *Telematics and Informatics Reports*, *10*, 100048. https://doi.org/10.1016/j.teler.2023.100048

Park, Y. J. (2013). Digital literacy and privacy behavior online. *Communication Research*, *40*(2), 215–236. https://doi.org/10.1177/0093650211418338

Parry, D. A., Davidson, B. I., Sewall, C. J. R., Fisher, J. T., Mieczkowski, H., & Quintana, D. S. (2021). A systematic review and meta-analysis of discrepancies between logged and self-reported digital media use. *Nature Human Behaviour*, 1–13. https://doi.org/10.1038/s41562-021-01117-5

Petty, R., & Cacioppo, J. (1986). *Communication and persuasion: Central and peripheral routes to attitude change*. Springer-Verlag. https://doi.org/10.1007/978-1-4612-4964-1

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

Rohrer, J. M. (2018). Thinking clearly about correlations and causation: Graphical causal models for observational data. *Advances in Methods and Practices in Psychological Science*, *24*(2), 251524591774562. https://doi.org/10.1177/2515245917745629

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. http://www.jstatsoft.org/v48/i02/

Schneider, F. M., Zwillich, B., Bindl, M. J., Hopp, F. R., Reich, S., & Vorderer, P. (2017). Social media ostracism: The effects of being excluded online. *Computers in Human Behavior*, *73*, 385–393.

Schreurs, L., Meier, A., & Vandenbosch, L. (2022). Exposure to the positivity bias and adolescents' differential longitudinal links with social comparison, inspiration and envy depending on social media literacy. *Current Psychology*. https://doi.org/10.1007/s12144-022-03893-3

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

Skinner, B. F. (2014). *Science and human behavior*. Pearson Education.

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

Spottswood, E. L., & Hancock, J. T. (2017). Should I share that?: Prompting social norms that influence privacy behaviors on a social networking site. *Journal of Computer-Mediated Communication*, *1*(2), 26. https://doi.org/10.1111/jcc4.12182

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

Stsiampkouskaya, K., Joinson, A., & Piwek, L. (2023). To like or not to like? An experimental study on relational closeness, social grooming, reciprocity, and emotions in social media liking. *Journal of Computer-Mediated Communication*, *28*(2), zmac036. https://doi.org/10.1093/jcmc/zmac036

Stubenvoll, M., Binder, A., Noetzel, S., Hirsch, M., & Matthes, J. (2022). Living is easy with eyes closed: Avoidance of targeted political advertising in response to privacy concerns, perceived personalization, and overload. *Communication Research*, 00936502221130840. https://doi.org/10.1177/00936502221130840

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 *Privacy online: Perspectives on privacy and self-disclosure*

in the social web (pp. 143–158). 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

van Ooijen, I., Segijn, C. M., & Opree, S. J. (2022). Privacy cynicism and its role in privacy decision-making. *Communication Research*, 00936502211060984. https://doi.org/10.1177/00936502211060984

Vanhove, J. (2021). Collinearity isn't a disease that needs curing. *Meta-Psychology*, *5*. https://doi.org/10.15626/MP.2021.2548

Venkatesh, Morris, Davis, & Davis. (2003). User acceptance of information technology: Toward a unified view. *MIS Quarterly*, *27*(3), 425. https://doi.org/10.2307/30036540

Vitak, J. (2012). The impact of context collapse and privacy on social network site disclosures. *Journal of Broadcasting & Electronic Media*, *56*(4), 451–470. https://doi.org/10.1080/08838151.2012.732140

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

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'*. https://CRAN.R-project.org/package=tidyverse