MUNI FSS

JOURNAL OF PSYCHOSOCIAL RESEARCH ON CYBERSPACE
CYBERPSYCHOLOGY

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), Article 1. https://doi.org/10.5817/CP2022-4-1

Getting the Privacy Calculus Right: Analyzing the Relations Between Privacy Concerns, Expected Benefits, and Self-Disclosure Using Response Surface Analysis

Murat Kezer[1], Tobias Dienlin[2], & Lemi Baruh[3]

[1] Department of Psychology, University of Oregon, USA
[2] Department of Communication, University of Vienna, Austria
[3] Department of Communication, Koç University, Turkey

Abstract

Rational models of privacy self-management such as privacy calculus assume that sharing personal information online can be explained by individuals' perceptions of risks and benefits. Previous research tested this assumption by conducting conventional multivariate procedures, including path analysis or structural equation modeling. However, these analytical approaches cannot account for the potential conjoint effects of risk and benefit perceptions. In this paper, we use a novel analytical approach called polynomial regressions with response surface analysis (RSA) to investigate potential non-linear and conjoint effects based on three data sets (N_1 = 344, N_2 = 561, N_3 = 1.131). In all three datasets, we find that people self-disclose more when gratifications exceed concerns. In two datasets, we also find that self-disclosure increases when both risk and benefit perceptions are on higher rather than lower levels, suggesting that gratifications play an important role in determining whether and how risk considerations will factor into the decision to disclose information.

Keywords: privacy calculus; privacy paradox; response surface analysis; online self-disclosure; anticipated benefits of self-disclosure; concerns about privacy; uses and gratifications

Editorial Record

First submission received:
September 29, 2021

Revisions received:
March 6, 2022
May 20, 2022

Accepted for publication:
July 1, 2022

Editor in charge:
Alexander P. Schouten

Introduction

In 2001, in a report aimed to outline how internet users' experience can be improved, Barry Brown from Hewlett Packard Laboratories observed "something of a 'privacy paradox'" (2001, p. 1): Surprisingly, despite voicing concerns about privacy and security, users gave up their privacy in exchange for only little gain (e.g., supermarket loyalty points). Since then, the concept of privacy paradox, which generally refers to a gap between reported concerns/attitudes about privacy and intentions/behavior, has been a central dimension of debates about privacy self-management (e.g., adoption of protective behavior, use of online services, disclosure of information; Barnes, 2006; Barth & de Jong, 2017; Baruh et al., 2017; Dienlin & Trepte, 2015; Kokolakis, 2017).

Extant literature offers a number of explanations for the privacy paradox phenomenon. One commonly cited explanation is that many of the studies observing the privacy paradox (Fogel & Nehmad, 2009; Shin & Kang, 2016; Taddicken, 2014) focus only on concerns or risk perceptions as a predictor of privacy management behavior. A commonly cited alternative to this approach is the privacy calculus model (Culnan & Armstrong, 1999), which

predicts that individuals' decisions about privacy management behavior involve weighing the expected negative consequences of sharing personal information along with the expected benefits of such behavior. Accordingly, individuals would be more likely to engage in behaviors such as signing up for a new social media platform or disclosing information when the anticipated benefits of doing so exceed the expected costs.

While privacy calculus has become a key concept in privacy literature, researchers have mainly used traditional statistical techniques (e.g., multiple regression) that may not be as informative about privacy calculus mechanism as relatively novel statistical approaches. In this study, we hence reinvestigate privacy calculus using a novel technique called Response Surface Analysis (RSA). RSA can put privacy calculus to a statistical test that is more closely aligned with the premise of privacy calculus by directly analyzing how the difference between concerns about privacy and anticipated benefits (e.g., benefits being higher than concerns) is related to online self-disclosure. Therefore, we reanalyze three data sets to determine if the privacy calculus indeed helps explain these data.

Privacy Calculus

An increasing number of studies offer evidence against the privacy paradox and in favor of the privacy calculus model: The privacy calculus is observed in different cultures (Trepte et al., 2017), on social networking sites (SNSs; Krasnova et al., 2010), or in e-commerce, health, and news consumption contexts (Bol et al., 2018). In addition, an empirical meta-analysis of k = 37 studies found a statistically significant relationship between privacy concerns and online self-disclosure (Baruh et al., 2017). Although the reported relation is small (r = −.13), it is not trivial and represents further evidence against the privacy paradox. Contrary to the assertion of the privacy paradox, this finding implies that people who are more concerned about their privacy disclose less information online. For instance, we would expect someone with a high level of concern about their privacy to be more likely to have private social media pages. Moreover, recent reviews of privacy management behavior suggest that perceived benefits may be a stronger predictor of disclosure intention and behavior than concerns about the anticipated negative outcomes (Barth & de Jong, 2017; Gerber et al., 2018).

However, the privacy calculus model faces both conceptual and methodical challenges. Conceptually, with its emphasis on a rational comparison of benefits and costs, the privacy calculus model builds on the "calculus of behavior" (Laufer & Wolfe, 1977, p. 35) and, more broadly, on the rational choice paradigm (Simon, 1955). As such, like other rational choice theories, the privacy calculus model has been criticized for assuming (or overstating) that individuals rationally weigh the risks and benefits of sharing information (Acquisti, 2004; Knijnenburg et al., 2017).

There are several reasons why, in privacy-related decisional contexts, individuals may not be able to engage in a fully rational calculus. First, in many contexts, privacy-related decisions are often automatic and driven by emotions (Masur, 2019; Zhang & Fu, 2020). Second, individuals' privacy-related decisions may often be based on "incomplete information" because both the risks and the benefits entail tangible as well as intangible dimensions (Acquisti, 2004). This impedes individuals' ability to make informed decisions. Specifically, not only will it be difficult for individuals to accurately estimate the costs of disclosing information (Acquisti, 2004; Acquisti et al., 2018; Barth & de Jong, 2017), but also lack of information about means of protection may prevent individuals from acting on their intentions (Brough & Martin, 2020; Park, 2013). Third, the concept of bounded rationality underscores that insofar as the human ability to engage in cognitive information processing is limited, privacy-related decisions will often rely on cognitive shortcuts. Reliance on cognitive shortcuts may result in several biases, such as optimistic bias (underestimating the risk of a negative outcome), status quo bias (preference for sticking to the current situation), or immediate gratification bias (Acquisti, 2004; Acquisti et al., 2018; Bandara et al., 2020; Hallam & Zanella, 2017). Participation in social networks, as their use is associated with social validation, connectivity, and self-presentation (Lee et al., 2013), is a prime example of how expectations about immediate gratifications may override the consideration of longer-term risks to one's privacy or security (Barth & de Jong, 2017; Debatin et al., 2009). Growing research on so-called dark patterns—interface designs that trick users into engaging in a behavior they did not mean to (Brignull, 2011)—underscores how such cognitive biases may be exploited by organizations to steer users into suboptimal privacy decisions (Nouwens et al., 2020; Waldman, 2020).

Related to these concerns about individuals' capacity for making rational calculations, in a recent review, Barth and De Jong (2017) argue that one explanation for why users may perform actions online which run counter to their privacy concerns might be that there are contexts when users do not make a risk calculation when thinking about privacy, but instead focus on the expected benefits. This may happen due to routinized engagement with a platform, resulting in suppression of considerations about privacy risks. It may also happen in contexts where

"value of desired goal outweighs risk assessment" (Barth & De Jong, 2017, p. 1048). Such contexts would include those within which the need for a service or product is so high that consideration of risks would be inconsequential and thereby unnecessary from the standpoint of the user. This would be the case when we consider simple conveniences in our lives, such as owning a smartphone or a credit card. Conversely, it is also possible that the expected benefits from a service or a product are insufficient to warrant a risk-benefit calculation, reducing the chances that risk considerations will factor into the decision to share information. Additionally, social compliance may be an important factor in reducing our ability to make autonomous decisions about disclosing information. This would be, for example, the case when disclosure is the norm for other members of a social network platform (Gerber et al., 2018; Lutz & Strathoff, 2014; Taddicken, 2014).

Reanalysing Privacy Calculus

Methodologically, one can question whether the studies supporting the privacy calculus have put it to a strict methodical test. For example, to test the hypotheses proposed by privacy calculus, most studies used multiple linear regression, path analysis, or structural equation modeling. A common approach is to model risks and benefits as predictors, with risks being negatively and benefits being positively associated with self-disclosure (e.g., Dinev & Hart, 2006; Trepte et al., 2017).

While useful for identifying the *isolated* linear impacts of risk and benefit perceptions of disclosure of personal information, the aforementioned conventional approaches cannot directly investigate the *conjoint* effects of both variables. Specifically, linear models cannot explicitly test whether the direction *of the difference* between risk and benefit perceptions influence disclosure (e.g., whether people disclose more if risks are larger than benefits or if benefits are larger than risks). This pattern would not be possible to test using multiple regression since it only provides the main effects of individual predictors (by controlling for the other predictors). In a similar vein, the effects of the respective *levels of perceived benefits and risks are* difficult to test via conventional methods. For instance, as discussed above, it may be the case that when expected benefits are at a high level, individuals are more likely to disclose personal information despite risk perceptions also being at a high level. Alternatively, as mentioned above, it is also possible that when individuals' benefit perceptions are low, they may not feel the need to evaluate risks before deciding not to share information. Unlike conventional methods such as multiple regression, RSA can test whether both predictors being at high levels (vs. at low levels) are statistically associated with the outcome.

Because we cannot answer these theoretically important questions using conventional analyses, in this study, we use a novel analytical technique called polynomial regression with RSA (Edwards & Parry, 1993). While the aim of this paper is primarily to introduce the application of RSA, as a novel statistical approach, to investigating privacy calculus, it also expands our theoretical understanding of privacy calculus by providing additional conceptual insights. First, through applying RSA, we achieve a test of the privacy calculus that is closer to its theoretical assumptions that the decision to share information is the result of the difference between levels of risk and benefit perceptions rather than being the result of the isolated influence of risk and benefit perceptions. Second, by allowing us to investigate at what respective levels of benefit and risk perceptions the difference between them is most likely to influence the decision to share information, RSA can improve our understanding of the mechanisms that may result in risk considerations not being related to information sharing. Because RSA is a novel type of analysis and not routinely used in Communication research, we first provide a brief overview of the technique. Then, we proceed by discussing how it helps advance the conceptual debates about privacy calculus and introduce our main hypothesis and our research question.

Response Surface Analysis

RSA is a fine-grained technique suitable for testing conjoint effects, in other words, how differences in two predictor variables (e.g., the difference between perceived risk and anticipated benefit) relate to an outcome variable (e.g., intention to disclose personal information in social media). RSA has often been used to investigate how two predictor variables relate to an outcome variable such as similarity effects (Cemalcılar et al., 2018) and is suitable to investigate a variety of conjoint effects.

Originally, the conjoint effects of two variables were tested using difference scores, which often take the form of algebraic, squared, or absolute differences. However, these approaches suffer from a variety of statistical and conceptual shortcomings, including (a) lower reliability than its components, (b) difficulty in interpretation, and

(c) confounding effects (for a detailed summary, see Edwards, 2002). RSA was developed to overcome these issues by simultaneously modeling the relationship between the outcome and the two predictors in a polynomial model, which encompasses both the differences and higher-order terms of these predictors (Edwards, 2002).

RSA starts with a *polynomial regression* (1). This polynomial regression contains the outcome variable (Z), linear and quadratic terms for the two predictors (X, X^2, Y, Y^2), and the interaction of the predictors (XY):

$$Z = b_0 + b_1X + b_2Y + b_3X^2 + b_4XY + b_5Y^2 + e. \quad (1)$$

As a result, the polynomial regression facilitates the testing of both linear and non-linear relations. However, rather than merely interpreting the coefficients of the polynomial regression, in RSA the polynomial regression coefficients are used to create a three-dimensional plot depicting how two predictors relate to the outcome, and to compute response surface values. In other words, these parameters are used to examine a *three-dimensional representation* of the relationship between the predictors and the outcome (Edwards & Parry, 1993; for an example, see Figure 1).

The response surfaces have several properties that can be used to make inferences. The *line of congruence* (LOC; blue line in Figure 1) is mathematically represented by the parameters a_1 (i.e., $b_1 + b_2$) and a_2 ($b_3 + b_4 + b_5$). It is the line where the two predictors have the same values (i.e., X = Y). When a_1 is significant but a_2 is not, LOC is linear. A positive a_1 indicates a linear additive effect, suggesting that the predicted outcome is higher when similar values of the predictors are on higher levels as compared to lower levels. When a_2 is significant, it means that LOC is curvilinear, producing the shape of a parabola. In other words, if both predictors increase, the outcome increases even stronger (i.e., exponentially).

Next, the *line of incongruence* (LOIC; red line in Figure 1) addresses situations when the two predictors have opposite values (i.e., X = −Y). LOIC is represented by the parameters a_3 (i.e., $b_1 - b_2$) and a_4 (i.e., $b_3 - b_4 + b_5$). A significant a_3 and a non-significant a_4 indicate that the line along the LOIC is linear and that the direction of the discrepancy (X > Y or Y > X) between the two predictor variables is important for the outcome. A positive a_3 suggests that the predicted outcome is at high levels when the first predictor is higher than the second predictor. A negative a_3 suggests that the outcome is at high levels when the second predictor is higher than the first predictor. A significant a_4 indicates that the LOIC is curvilinear, producing the shape of a parabola.

For an overview of the coefficients' meaning, see Table 1. For a more comprehensive explanation and visual representations of the surface parameters, see Nestler et al. (2019, p. 294). For a tutorial, see Edwards and Parry (1993).

Table 1. *Meaning of the Coefficients.*

Coefficient	Calculation	Meaning
Polynomial Regression		
b_1		Linear effect of predictor X.
b_2		Linear effect of predictor Y.
b_3		Curvilinear effect of predictor X.
b_4		Interaction of predictor X and predictor Y.
b_5		Curvilinear effect of predictor Y.
Response Surface		
a_1	$b_1 + b_2$	The outcome is higher when values of the predictors are on higher levels.
a_2	$b_3 + b_4 + b_5$	The outcome value is highest for a specific X-Y pair, but is lower for other combinations of the predictors.
a_3	$b_1 - b_2$	The outcome is higher when predictor X is on a higher level than predictor Y.
a_4	$b_3 - b_4 + b_5$	The outcome is higher when predictors are at similar values.

Note. For the interpretation of the response surface parameters, we assume that all other parameters are not significant. For instance, when interpreting a significant a_1, we assume that a_2, a_3, and a_4 are not significant. Also, a significant a_4 is not the only condition for a congruence effect, it also requires a non-significant a_5, which is beyond the scope of this article.

Combining Privacy Calculus and Response Surface Analysis

The use of RSA to investigate privacy calculus enables researchers to pose and answer important and interesting questions. For example, does the privacy calculus only take place once costs and/or benefits reach a certain magnitude? If so, at what levels of concerns and gratifications?

Furthermore, this methodology is informative for different explanations of the privacy paradox summarized above. Consider, for example, how "incomplete information" may both result in an underestimation of risks and/or a lack of knowledge regarding the implementation of effective protective measures. In RSA, these two potential consequences of "incomplete information" would, however, manifest themselves differently: When individuals underestimate risks, we would expect a positive relationship between the size of the difference between benefits (high) and risks (suppressed, low) and disclosure behavior. Within the RSA framework, we would observe that while benefits have a positive and linear main effect (significant b_1 and non-significant b_3–b_5), concerns do not have a main effect (non-significant b_2); furthermore, the line of incongruence would be linear and positive (significant a_3 and non-significant a_4), but this effect would be driven only by the benefits (significant b_1 and non-significant b_2). However, when individuals lack procedural knowledge about protecting themselves, we could expect to see disclosure behavior even when there is only a negligible difference between perceived benefits and risks. In RSA terms, we would expect that both benefits (b_1) and concerns (b_2) are positive and significant while the other predictors (b_3–b_5) are non-significant, but because concerns cannot translate into protective behavior, the difference between benefits (b_1) and concerns (b_2) would be less likely to predict behavior, leading to a non-significant line of incongruence (i.e., a_3 and a_4).

As a second example, let us revisit what Barth and De Jong describe as contexts where the expected value is so high that individuals do not consider the risks. What is important to note here, though, is the qualitative distinction between (a) "not considering" risks because the benefits are very high and (b) suppressing concerns about risks because there is no viable option for acting otherwise—a pattern related to what has been called privacy fatigue (Choi et al., 2018), privacy apathy (Hargittai & Marwick, 2016), or privacy cynicism (Hoffmann et al., 2016; van Ooijen et al., 2022). In the former, risk estimations might be low and potentially have no main effect on disclosure behavior, while benefits are high and may have a positive main effect. In RSA terminology, this model would translate to a linear and positive effect of benefits (significant b_1) while all of the other parameters (b_2–b_5 and a_1–a_4) are non-significant. In the latter case, it can be expected that disclosure behavior will be positively associated with a congruent increase in both benefit and risk perceptions, represented by a negative and non-linear line of incongruence with no main effects of the predictors (i.e., non-significant a_1–a_3, significant a_4; non-significant b_1–b_2 and significant b_3–b_5).

These examples suggest that RSA can contribute to the literature on privacy calculus in several ways. Notably, there is a growing body of literature that challenges the rationality assumption to investigate privacy management behavior. Such studies incorporate factors such as cognitive biases and affective states into the calculus, which would also be possible to test using RSA methodology (Kehr et al., 2015; Wilson & Valacich, 2012; Zhang & Fu, 2020). To untangle the intricate relationship of perceived benefits and concerns with online self-disclosure, in this study, we focus on the line of incongruence. Specifically, we formulate the following hypothesis:

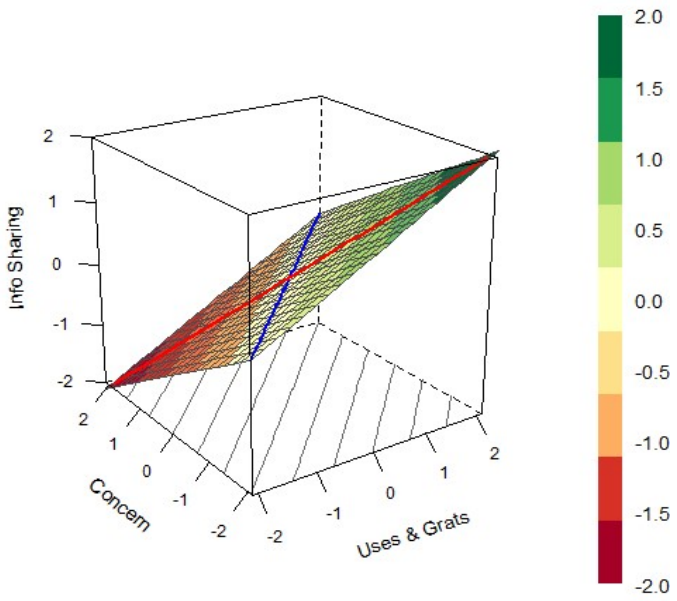
H1: People are more likely to share information when perceived risks are lower than perceived benefits.

Accordingly, we expect a significant linear line of incongruency along with a non-significant line of congruence (i.e., significant a_3 and non-significant a_1, a_2, and a_4). Figure 1 visualizes this relationship. For instance, we expect that sharing behavior is at its highest (i.e., +2) for a participant that scored +2 on benefits and −2 on concerns, whereas the outcome is at its lowest (i.e., −2) for another participant that scored −2 on benefits and +2 on concerns. The same pattern can be observed for any pair of scores. A linear LOIC (as well as a nonsignificant LOC) informs us that this comparison is statistically significant.

The examples discussed above also raise the possibility that the relationship between these two predictors and sharing information will vary as a function of whether the perceived risks and benefits are low, moderate, or high. In this light, we additionally aim to investigate the following research question:

RQ1: At what levels of perceived benefits and risks does the difference influence disclosure the most?

Figure 1. *Example Plot for Assumed Relationships.*



Note. The x-axis represents Uses & Gratifications, the y-axis represents concerns about privacy, and the z-axis represents sharing personal information online. The values of variables come from a hypothetical distribution (i.e., z-scores). LOIC is the red line and represents cases where the predictors have opposite values. According to privacy calculus, we expect that it has a positive slope: If gratifications are larger than benefits, self-disclosure increases. LOC is the blue line, where both concern and Uses & Gratifications have the same values.

Methods

Data Analysis

We analyzed the data in R (R Core Team, 2020) using the package RSA (Schönbrodt, 2017). The factorial validity of all scales was tested by confirmatory factor analysis (CFA) using the raw data and *lavaan* package in R (Rosseel, 2012), and the model fits were evaluated based on the guidelines that can be found in Kline (2015). We estimated the RSA after centering the predictors around their mid-scale point, whose composite scores were computed by taking the average of the items indicated by the CFA models. Centering around mid-scale facilitates interpretation of the coefficients and deals with multicollinearity (Aiken et al., 1991; Edwards & Parry, 1993). The regressions were conducted using ordinary least squares, which require that residuals are normally distributed. Analyses showed that the residuals of study 2 were not normally distributed. Because RSA uses robust estimators, which help address non-normality (Pek et al., 2018), we are nonetheless optimistic that the violation of the normality assumptions is not problematic. The data, the items, the analysis scripts, and a detailed documentation of the results, and the descriptive summary of the variables can be found in the online supplementary materials: (https://osf.io/sy2az/?view_only=1394c169381845408f8d3134db535b3a).

Since we used secondary data, we were not able to conduct a priori power analysis. However, a sensitivity power analysis conducted using G*Power 3.1 (Faul et al., 2009) with five predictors for polynomial regression (i.e., R^2 going from two to five predictors) indicated that we could detect an effect size as small as f_2 = .028 (i.e., R_2 = .027), f_2 = .017 (i.e., R_2 = .017), f_2 = .008 (i.e., R_2 = .008) for Dataset 1, 2, and 3, respectively, with 80% power at α = 0.05. Furthermore, the observed effect sizes across the datasets were greater than the values indicated by the sensitivity power analyses (see Table 2 for the effect sizes).

Dataset 1

Procedure and Participants

The data come from an online survey, conducted online via Qualtrics survey platform, focusing on the relationship between personality traits and social media use tendencies.

A total of 344 students at a private university in Turkey during April in 2015 completed the survey. The average age was 21.20 years (*SD* = 2.25), 60% were female, and 30% reported having a college or graduate degree.

Measures

Anticipated benefits were captured with *uses and gratifications of Twitter scale* (Baruh, 2010; Chen, 2011). The current study measured four dimensions of Twitter uses and gratifications: Using Twitter to (a) network with others (e.g., *to meet new people*); (b) satisfy social curiosity (e.g., *to learn about daily lives of other people*); (c) self-express (e.g., *to make people understand me better*); and to (d) maintain relationships (e.g., *to keep in contact with family and friends*). All items described above were measured on a 5-point scale (1 = *strongly disagree* to 5 = *strongly agree*). A hierarchical measurement model including all 15 items (M = 2.75, SD = 0.72) and four dimensions showed good factorial validity, $\chi^2(86) = 229.48$, $p < .001$, CFI = .95, RMSEA = .07, 90% CI [.06, .08], SRMR = .07. The reliability for the second-order factor (i.e., general UG factor) was high ($\omega = .90$).

Perceived risks of disclosing personal information are operationalized as *concerns about privacy*, which was assessed with 7 items adapted from existing privacy scales on a 5-point scale (e.g., *I worry about sharing information with more people than I intend to*; Baruh & Cemalcılar, 2014; Stieger et al., 2013). We ran a series of CFAs to investigate the factorial structure of the scale. Three items were removed due to insufficient factor loadings. The resulting scale with 4 items (M = 3.11, SD = 0.75) showed acceptable levels of factorial validity, $\chi^2(2) = 19.57$, $p < .001$, CFI = .93, RMSEA = .16, 90% CI [.10, .23], SRMR = .04. Reliability was also at an acceptable level ($\omega = .73$).

The dependent variable, sharing information on Twitter, was assessed using eight items adapted from the *self-disclosure index* (Miller et al., 1983). Respondents were asked to rate, on a 4-point scale (1 = *never* to 4 = *more than once a day*), the frequency with which they would tweet about various topics about themselves (e.g., *my personal habits*). A measurement model with 6 items (M = 1.99, SD = 0.48) showed just acceptable factorial validity, $\chi^2(9) = 58.18$, $p < .001$, CFI = .93, RMSEA = .13, 90% CI [.10, .16], SRMR = .04 and reliability was high ($\omega = .84$).

Dataset 2

Procedure and Participants

The data come from an online experiment conducted in Germany during the fall term of 2017, which analyzed the privacy calculus using actual behavioral data (for more details on the study, see Dienlin et al., 2020). The field phase of the experiment lasted for one week. On an authentic website, participants were invited to discuss a current political topic (i.e., how to prevent terrorist attacks). Afterwards, participants answered a follow-up questionnaire about privacy concerns and obtained gratifications.

The final data set consists of 561 participants, of which 51% were female. The average age was 46.20 years (SD = 15.60), and 29% reported having a college degree.

Measures

Anticipated benefits of using the social networking site were captured with a 15-item scale of *specific uses and gratifications*. The scale consisted of five dimensions (informativeness, relevance, participation, meaningfulness, help). One example item is *Using the participation platform it has been possible for me to learn things I would not otherwise have noticed.* The scale had a 7-point answer format, with options ranging from 1 = *completely disagree* to 7 = *completely agree* (M = 4.71, SD = 1.00). Factorial validity was okay, $\chi2(85) = 448.03$, $p < .001$, CFI = .93, RMSEA = .09, 90% CI [.08, .10], SRMR = .06 and reliability was good ($\omega = .95$).

The perceived risks of disclosing personal information were operationalized with a 7-item scale of *online privacy concerns*. One example item is *Using the participation platform I had concerns about my privacy.* The scale had a 7-point answer format, with options ranging from 1 = *completely disagree* to 7 = *completely agree* (M = 3.45, SD = 1.25). The scale showed good factorial validity, $\chi2(14) = 44.22$, $p < .001$, CFI = .99, RMSEA = .06, 90% CI [.04, .09], SRMR = .01 and reliability was high ($\omega = .92$).

The dependent variable measured the number of words, likes, and dislikes shared on the website, which was then log-scaled (M = 1.92, SD = 2.28).

Dataset 3

Procedure and Participants

The data come from an online experiment conducted in the Netherlands during the fall term of 2017 that aimed to examine privacy calculus using hypothetical scenarios (Bol et al., 2018). Participants were instructed to read different scenarios in randomly assigned conditions and to look for information using a search engine, followed by visiting a website. After the experiment, participants filled out an online survey about perceived concerns and benefits and willingness for future self-disclosure (for more details about the experiment, see Bol et al., 2018).

The final sample consisted of 1131 participants (M_{age} = 56.00, SD_{age} = 16.30; 50% female, 37% higher education), and was representative of Dutch population.

Measures

Anticipated benefits were assessed by eight items, answered on a 7-point scale ranging from 1 = *strongly disagree* to 7 = *strongly agree,* either generated by the authors or based on the previous literature (*M* = 3.01, *SD* = 1.35). One sample item was *I find sharing my personal information with [health/shopping/news] websites useful in my daily life.* The factorial validity of the scale was okay, $\chi^2(20) = 480.53$, $p < .001$, CFI = .94, RMSEA = .13, 90% CI [.14, .15], SRMR = .04. Reliability was high (ω = .95).

Privacy concerns were assessed by 5 items adopted from Baek and Morimoto (2012). Items were on a 7-point scale ranging from 1 = *strongly disagree* to 7 = *strongly agree* (*M* = 5.25, *SD* = 1.35). One sample item was *When I visit [health/shopping/news] websites, I have the feeling that others keep track of where I click*. The scale showed good factorial validity, $\chi^2(5) = 23.81$, $p < .001$, CFI = .99, RMSEA = .06, 90% CI [.04, .08], SRMR = .01. Reliability was high (ω = .95).

To assess *willingness for future online self-disclosure*, participants were asked to report how likely it is for them to share personal information (e.g., their name) if they visited a similar website in the future on a 7-point scale (*M* = 2.24, *SD* = 1.28). The scale showed good factorial validity, $\chi^2(21) = 117.33$, $p < .001$, CFI = .99, RMSEA = .05, 90% CI [.06, .08], SRMR = .03. Reliability was high (ω = .92).

Results

The data were analyzed using RSA.[1] RSA requires that there be sufficient numbers of cases representing all possible combinations of two predictors (i.e., risks > benefits; benefits > risks; risks ≈ benefits; Shanock et al., 2010). Across all datasets, we fulfill that condition. For example, for Dataset 1, in 47.7% of the cases, perceived benefits were lower than privacy concerns, in 21.8% of the cases perceived benefits exceeded privacy concerns while in 30.5% of the cases perceived benefits and privacy concerns were equal (see online supplementary materials for all distributions of congruent and incongruent cases). In addition, because RSA is based on polynomial regression, another requirement is that residuals are normally distributed. Analyses revealed that the residuals of Dataset 2 were not normally distributed. To investigate whether the results are affected by the non-normally distributed residuals, we also conducted a bootstrapped RSA with 1000 samples. This technique is a valid strategy to effectively handle non-normally distributed residuals (Pek et al., 2018). The bootstrapped results were closely aligned with the regular ones (e.g., the same effects were significant). Because RSA is conducted with robust estimators and hence robust to violations of the normality assumption of residuals, and because results were virtually identical, in what follows we report the results of the regular RSAs. The results of the bootstrapped RSA can be found in the online supplementary materials. Table 2 presents the coefficients for polynomial regression and surface parameters.

Our focus is on the incongruence between risk and benefit perceptions (i.e., risks > benefits vs. benefits > risks). In RSA, this is represented by a_3 and a_4. As explained above, a significant a_3 with a non-significant a_4 shows that the incongruence effect is significant and linear (i.e., not curvilinear). As expected, in Dataset 2, this is exactly the pattern we observe. That is, a_3 was positive (i.e., .50) while other surface parameters were non-significant. This finding suggests that the number of words shared by participants was greater when perceived benefits exceeded perceived risks. For example, the predicted value of the number of words shared is around 2.15 (*M* = 1.92) for someone who scores 6 (on a 7-point scale) on benefits and who scores 4 (on a 7-point scale) on concerns about privacy; whereas the predicted value of the outcome is around 1.12 for someone with the opposite pattern (also, see Figure 2).

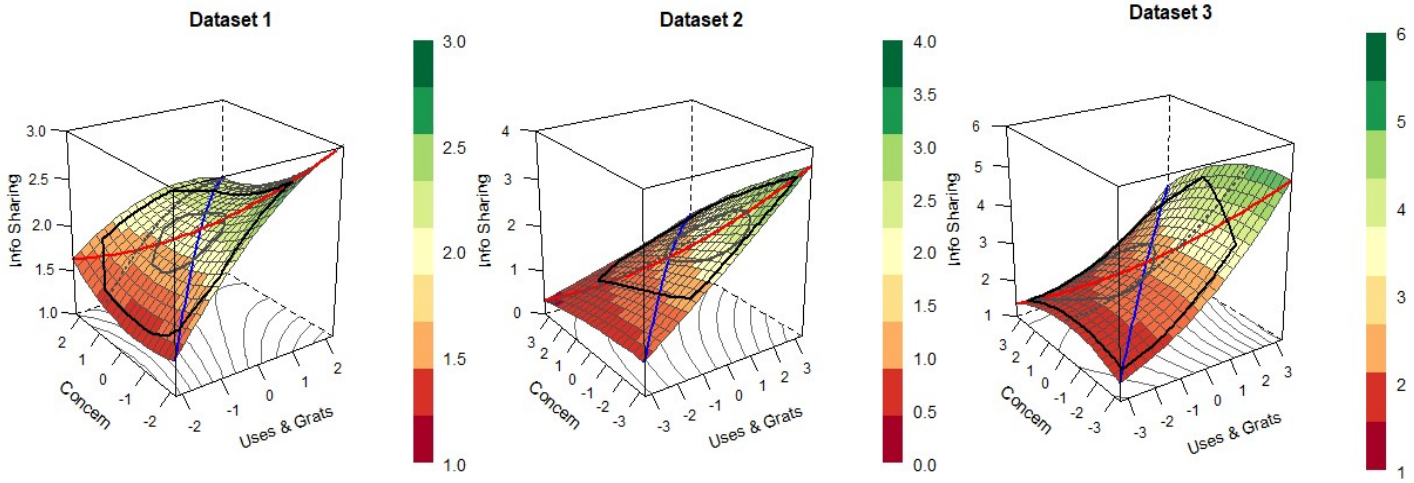
Table 2. *Polynomial Regression Coefficients and Surface Parameters.*

		Dataset 1			Dataset 2			Dataset 3		
Label	Description	*b*	*SE*	*p*	*b*	*SE*	*p*	*b*	*SE*	*p*
Polynomial Model										
b_1	Benefit	**.24**	0.04	< .001	**.30**	0.10	.004	**.44**	0.06	< .001
b_2	Concern	**−.07**	0.04	.037	**−.20**	0.08	.013	**−.13**	0.05	.008
b_3	Benefit^2	−.05	0.03	.086	.01	0.05	.933	**.05**	0.03	.043
b_4	Benefit × Concern	−.06	0.04	.149	−.04	0.05	.411	−.03	0.02	.121
b_5	Concern^2	.04	0.03	.165	−.01	0.04	.831	**−.04**	0.02	.004
Response Surface Parameters										
a_1	$b_1 + b_2$	**.17**	0.05	< .001	.10	0.14	.492	**.31**	0.08	< .001
a_2	$b_3 + b_4 + b_5$	−.07	0.05	.159	−.05	0.09	.595	−.03	0.04	.528
a_3	$b_1 - b_2$	**.32**	0.06	< .001	**.50**	0.12	< .001	**.58**	0.08	< .001
a_4	$b_3 - b_4 + b_5$	.05	0.07	.434	.04	0.07	.590	.04	0.03	.136

Note. Statistically significant coefficients are in bold. The dependent variables are self-reported personal information sharing on Twitter, the number of words posted on a website, and the willingness for future online self-disclosure for Dataset 1, 2, and 3, respectively. The R^2 values for Dataset 1, 2, and 3, are .176, .046, and .185, respectively; all *p*s < .001.

In Dataset 1 and 3, findings were similar to one another but slightly different from the findings in Dataset 2. Both LOC and LOIC were positive and linear (i.e., positive a_1 and non-significant a_2; positive a_3 and non-significant a_4). As in Dataset 2, the positive a_3 indicates that participants reported (the willingness for) sharing more information online when their anticipated benefits were higher than their concern for their privacy (compared to the other way around). At the same time, unlike in Dataset 2, the positive a_1 indicates that the outcome variables (i.e., self-reported self-disclosure on Twitter in Dataset 1 and the willingness for future online self-disclosure in Dataset 3) were greatest when both benefits and concerns about privacy were high (see Table 2 and Figure 1 for the parameters and plots).

Figure 2. *Response Surfaces for Dataset 1–3.*



Note. X-axis shows perceived benefits of online disclosure, y-axis shows concerns about privacy, z-axis shows specific outcome variables. The bag plots, as displayed on the surfaces, indicate the location, spread, correlation, skewness, and tails of the data (Rousseeuw et al., 1999), analogous to boxplots. The area inside the larger bag contains half of the observations, and the rest are located in the region between the inner and outer bag.

The findings suggest that, overall, the willingness for sharing information was highest when both the benefits and risks were highest, and the benefits were greater than the concerns compared to the opposite pattern. For example, in Dataset 1, the predicted value of information sharing on Twitter is around 2.26 (*M* = 1.99) for someone who scores 4 (on a 5-point scale) on benefits and who scores 3 (on a 5-point scale) on concerns about privacy; whereas the predicted value of the outcome is around 2.04 for someone with the opposite pattern (see Figure 2). In a similar fashion, in Dataset 3, the predicted value of the willingness for the future online self-disclosure is around 3.76 (*M* = 2.24) for someone who scores 6 (on a 7-point scale) on benefits and who scores 4 (on a 7-point scale) on concerns about privacy; whereas the predicted value of the outcome is around 2.43 for someone with the opposite pattern, which is still above the mean level, indicating the additivity effect of benefits and concerns.

Discussion

The present study reanalyzed three datasets by applying a novel analytical technique called RSA to understand better the relationship of anticipated benefits and risks of information sharing with online self-disclosure. While techniques like linear regression test how the benefits and concerns separately predict online self-disclosure, they do not offer a direct test of the main premise of the privacy calculus model, which predicts that self-disclosure depends on the *difference* between these variables, or more precisely, whether perceived benefits exceed perceived risks. The use of RSA allowed us to explicitly test how the *difference* between the benefits and concerns was associated with online self-disclosure.

Consistent with our expectations, the findings demonstrate that individuals are more likely to engage in online self-disclosure when their anticipated benefits exceed their concerns about privacy. In addition, the findings from Datasets 1 and 3 indicate that online self-disclosure is greatest when both benefits and concerns are high. This finding underscores the importance of perceived benefits as a factor that qualifies the nature of the risk-benefit calculation in privacy calculus because it implies that, unless they expect a benefit, users will not engage in disclosure just because it is not risky to do so. In other words, benefit considerations may act as a steppingstone for the privacy calculus in the sense that users will potentially first consider whether there is sufficient benefit from the act of disclosure and then will evaluate potential risks only if they expect benefits. Conversely, as we will further discuss below, there may also be contexts within which expected benefits are so important that risk considerations are suppressed. These possibilities have several important implications for research on privacy calculus. First, it supports the need to apply a more situational perspective (Masur, 2019) in assessing the relative role that risk-benefit considerations play in predicting disclosure. Second, it points to the need to collect more finely grained data that can help investigate in further detail the risk-benefit evaluation processes of individuals (e.g., the sequence with which they are considered in varying contexts). Third, it underlines the importance of decisions regarding the selection of disclosure behavior that will be treated as the dependent variable. Specifically, especially in studies that investigate the linear relationship between risk perceptions/concerns and disclosure behavior, researchers should be cognizant of the possibility that for disclosure behaviors that are not perceived to be highly beneficial, risk perceptions will be less likely to be a factor that predicts the behavior.

More generally, these findings suggest that a privacy calculus that emphasizes the relationship between the concerns and benefits is a more suitable model to explain self-disclosure than the privacy paradox, which overlooks the anticipated benefits of self-disclosure. This is also consistent with the findings of a recent study that used an elaboration likelihood model to investigate privacy calculus and privacy fatigue within the context of a health application (Zhu et al., 2021). The authors found that while perceived benefits of sharing personal information was positively associated with disclosure intentions, this relationship was reversed for privacy concerns. More importantly, perceived benefits were a stronger predictor of disclosure intentions than privacy concerns (Zhu et al., 2021).

One potential explanation of this pattern of results is that having "incomplete information" regarding benefits and privacy concerns promotes high levels of self-disclosure either because estimation of risk is inaccurate, or because individuals have inadequate information regarding how to protect their privacy in online settings. For instance, research shows that although older individuals (i.e., 65+) are concerned about their privacy, they lack the knowledge and skills to protect it (Kezer et al., 2016). Moreover, in a context where individuals perceive disproportionately more benefits of sharing personal information, individuals may fail to conduct a risk assessment. Alternatively, in contexts where individuals habitually spend a considerable amount of time online, they may not be cognizant of the risks of self-disclosure. Similarly, in such contexts, it is possible to observe norms that compel self-disclosure, which may be leading them to suppress or disregard their concerns about privacy. We recommend that future research models these factors explicitly, so that our theoretical explanations can be tested empirically.

In line with the immediate gratification bias (Acquisti, 2004), another possible explanation for why individuals are influenced by the benefits of self-disclosure more than by concerns for privacy is that self-disclosure is intrinsically rewarding (Tamir & Mitchell, 2012). That is, humans feel rewarded when sharing information about themselves, in the same way when satisfying primal needs such as hunger. Similarly, research shows that we like people who disclose to us and vice versa (Collins & Miller, 1994). Indeed, from an evolutionary standpoint, self-disclosure brings about many adaptive advantages such as strengthening social relationships and receiving feedback from others about one's self (Dunbar, 1997).

In conclusion, our findings in all three datasets indicate that the anticipated benefits of self-disclosure outweigh concerns about privacy for individuals to engage in online self-disclosure. Therefore, we posit that people engage in a privacy calculus where online self-disclosure takes place only when benefits exceed concerns. In other words, there is a privacy calculus, and the benefits are more important.

Limitations

Although in this paper we hypothesize that privacy concerns and expected benefits influence self-disclosure and not vice versa, this assumption is based purely on theoretical grounds, because all three studies do not allow for causal statements. In particular, the correlational nature of the current research does not eliminate the effect of unobserved factors on both predictors and outcomes. For instance, participants' mood at the time of data collection may have impacted the results. Someone who is in a highly positive mood may have perceived higher benefits and may have disclosed more as a result of their mood.

RSA allows us to statistically compare the role of both benefits and costs. As a result, we can now state that people are more likely to disclose if the benefits actually exceed the costs. At the same time, we still do not know whether participants explicitly compare benefits to costs. It might be that this process takes place implicitly, for example via heuristics (Sundar et al., 2013). Similarly, RSA may not be a suitable technique to test all models related to privacy calculus. Nevertheless, RSA can be a useful analytical tool when including additional predictors and covariates, such as declarative and procedural privacy literacy.

As discussed above, across two datasets, in addition to our main finding, we observed that levels of self-disclosure increased if both benefits and concerns were on higher levels. However, this relationship was not replicated in the second dataset. Therefore, this finding might not be generalizable and robust. Future research with the same research design as in the second dataset is required to provide stronger evidence to support or to reject this association.

We have explained self-disclosure using two variables. However, other variables likely also explain self-disclosure (e.g., mood, context, or culture), which could attenuate the effects reported here. Hence, the coefficients might be overestimated. On the other hand, because response surface analysis is based on polynomial regression analysis using manifest variables, it is not possible to partial out error variance by using latent factors, which is why the effects might also be underestimated.

Our measures for concerns and benefits in Dataset 1 somewhat differed in their degree of specificity. While we measured gratifications obtained from using Twitter to operationalize positive aspects of self-disclosure, the scale used to measure negative attitudes toward self-disclosure touched upon more general concerns about one's privacy. Even though such general concerns may encompass specific concerns, the results would be more precise with predictors measured at similar levels of specificity. Acknowledging the shortcomings of the secondary datasets used in the present research, we believe that future research should pay more attention to the measurement of risks and benefits of self-disclosure such that both predictors should be measured on the same level.

In a similar vein, the measures employed to assess risks and benefits of self-disclosure in Dataset 3 evaluate risks and benefits of self-disclosure at a general level for the websites that the participants visited. A measurement of the risks and benefits for the specific task that they were asked to complete would also be informative so as to understand how self-disclosure in a specific situation may deviate from a general privacy calculus. Thus, researchers should also investigate specific situations across different contexts (e.g., Twitter vs Instagram) to reveal whether (or how) assessments of general and specific risks and benefits of self-disclosure are related to self-disclosure.

Another potential issue with our use of secondary datasets for this paper concerns the content validity of the disclosure items we used as the dependent variable. In Dataset 1, we used a self-reported frequency with which respondents tweeted about different topics about themselves. In Dataset 2, disclosure was operationalized using the number of words, likes and dislikes shared on the website. In Dataset 3, disclosure was assessed with items asking intentions to share various information about themselves. In general, the extant literature on self-disclosure distinguishes between two dimensions of disclosure: breadth and depth. The former refers to the quantity of information, the number of utterances, or the number of topics, whereas the latter refers to the level of sensitivity (i.e., how private the information is; Collins & Miller, 1994; Greene et al., 2006). Research indicates that these two dimensions not only differ from each other in terms of their potential predictors but also in terms

of how they may influence relational outcomes (Baruh & Cemalcılar, 2018; Bazarova & Choi, 2014; Orben & Dunbar, 2017). Unfortunately, due to lack of access to a dataset that measured depth, all the datasets we used were primarily about the breadth of disclosure; nevertheless, the RSA technique can readily be applied to studies that investigate predictors of the depth of disclosure.

Our study was not preregistered. Two of the datasets we used come from studies that have already supported the privacy calculus. We recommend utilizing RSA while conducting novel, preregistered studies using new data. We emphasize the need to run a priori power analysis. Response surface analyses are based on polynomial regression; consequently, they need two to three times the usual sample size (Aiken et al., 1991).

Implications and Conclusion

Despite the study's limitations, the findings suggest that the anticipated benefits contribute more to the decision to share personal information in online settings, using a relatively more precise statistical method (i.e., RSA). Importantly, online self-disclosure seems to be at its highest when the perceived benefits exceed the concerns about privacy.

Finally, one of the most important implications of the study lies in its methodology. The study underscores the potential utility of the RSA technique in further exploring how and why people engage in self-disclosure, even when they are highly concerned about the consequences of such exposure. We recommend that future research now takes into consideration additional key predictors such as literacy, trust, and affect, to further contextualize the nuances of online self-disclosure.

Footnotes

[1] We also conducted condition-based regression analysis (CRA; Humberg et al., 2018) for each dataset. CRA is similar to RSA in that, like RSA can, it also tests whether one predictor being greater than the other predictor affects the outcome or only one predictor accounts for the results. Applying CRA in our datasets, we found the same results as with the RSA, suggesting that online self-disclosure is higher when anticipated benefits of self-disclosure exceed perceived concerns about privacy. It should be noted that although the finding for Dataset 1 was in the same direction as the findings in the other datasets, it was not statistically significant. See online supplementary material for the analyses and results.

Conflict of Interest

The authors do not have any conflicts of interest to report.

Authors' Contribution

Murat Kezer: conceptualization, methodology, formal analysis, data curation, writing – original draft, writing – review & editing, visualization. **Tobias Dienlin:** methodology, formal analysis, data curation, writing – original draft, writing – review & editing, visualization**. Lemi Baruh:** conceptualization, methodology, data curation, writing – original draft, writing – review & editing.

References

Acquisti, A. (2004). Privacy in electronic commerce and the economics of immediate gratification. In *Proceedings of the 5th ACM Conference on Electronic Commerce - EC '04* (pp. 21–29). https://doi.org/10.1145/988772.988777

Acquisti, A., Adjerid, I., Balebako, R., Brandimarte, L., Cranor, L. F., Komanduri, S., Leon, P. G., Sadeh, N., Schaub, F., Sleeper, M., Wang, Y., & Wilson, S. (2018). Nudges for privacy and security: Understanding and assisting users' choices online. *ACM Computing Surveys*, *50*(3), Article 44. https://doi.org/10.1145/3054926

Aiken, L. S., West, S. G., & Reno, R. R. (1991). *Multiple regression: Testing and interpreting interactions*. SAGE Publications.

Baek, T. H., & Morimoto, M. (2012). Stay away from me. *Journal of advertising, 41*(1), 59-76. https://doi.org/10.2753/JOA0091-3367410105

Bandara, R., Fernando, M., & Akter, S. (2020). Explicating the privacy paradox: A qualitative inquiry of online shopping consumers. *Journal of Retailing and Consumer Services*, *52*, Article 101947. https://doi.org/10.1016/j.jretconser.2019.101947

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

Barth, S., & de Jong, M. D. T. (2017). The privacy paradox – Investigating discrepancies between expressed privacy concerns and actual online behavior – A systematic literature review. *Telematics and Informatics*, *34*(7), 1038–1058. https://doi.org/10.1016/j.tele.2017.04.013

Baruh, L. (2010). Mediated voyeurism and the guilty pleasure of consuming reality television. *Media Psychology*, *13*(3), 201–221. https://doi.org/10.1080/15213269.2010.502871

Baruh, L., & Cemalcılar, Z. (2014). It is more than personal: Development and validation of a multidimensional privacy orientation scale. *Personality and Individual Differences, 70*, 165–170. https://doi.org/10.1016/j.paid.2014.06.042

Baruh, L., & Cemalcılar, Z. (2018). When more is more? The impact of breadth and depth of information disclosure on attributional confidence about and interpersonal attraction to a social network site profile owner. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace*, *12*(1), Article 1. https://doi.org/10.5817/CP2018-1-1

Baruh, L., Secinti, E., & Cemalcılar, 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., & Choi, Y. H. (2014). Self-disclosure in social media: Extending the functional approach to disclosure motivations and characteristics on social network sites. *Journal of Communication*, *64*(4), 635–657. https://doi.org/10.1111/jcom.12106

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

Brignull, H. (2011, November 1). Dark patterns: Deception vs. honesty in UI design. *A List Apart*. https://alistapart.com/article/dark-patterns-deception-vs-honesty-in-ui-design/

Brough, A. R., & Martin, K. D. (2020). Critical roles of knowledge and motivation in privacy research. *Current Opinion in Psychology*, *31*, 11–15. https://doi.org/10.1016/j.copsyc.2019.06.021

Brown, B. (2001). *Studying the internet experience* (HPL-2001-49). HP Laboratories Bristol. https://hplabs.itcs.hp.com/techreports/2001/HPL-2001-49.html

Cemalcılar, Z., Baruh, L., Kezer, M., Kamiloglu, R. G., & Nigdeli, B. (2018). Role of personality traits in first impressions: An investigation of actual and perceived personality similarity effects on interpersonal attraction across communication modalities. *Journal of Research in Personality*, *76*, 139–149. https://doi.org/10.1016/j.jrp.2018.07.009

Chen, G. M. (2011). Tweet this: A uses and gratifications perspective on how active Twitter use gratifies a need to connect with others. *Computers in Human Behavior*, *27*(2), 755–762. https://doi.org/10.1016/j.chb.2010.10.023

Choi, H., Park, J., & Jung, Y. (2018). The role of privacy fatigue in online privacy behavior. *Computers in Human Behavior*, *81*, 42–51. https://doi.org/10.1016/j.chb.2017.12.001

Collins, N. L., & Miller, L. C. (1994). Self-disclosure and liking: A meta-analytic review. *Psychological Bulletin*, *116*(3), 457–475. https://doi.org/10.1037/0033-2909.116.3.457

Culnan, M. J., & Armstrong, P. K. (1999). Information privacy concerns, procedural fairness, and impersonal trust: An empirical investigation. *Organization Science*, *10*(1), 104–115. https://doi.org/10.1287/orsc.10.1.104

Debatin, B., Lovejoy, J. P., Horn, A.-K., & Hughes, B. N. (2009). Facebook and online privacy: Attitudes, behaviors, and unintended consequences. *Journal of Computer-Mediated Communication*, *15*(1), 83–108. https://doi.org/10.1111/j.1083-6101.2009.01494.x

Dienlin, T., Bräunlich, K., & Trepte, S. (2020). *How Do Like and Dislike Buttons Affect Communication? Testing the Privacy Calculus in a Preregistered One-Week Field Experiment* [Preprint]. SocArXiv. https://doi.org/10.31235/osf.io/7kjf2

Dienlin, T., & Trepte, S. (2015). Is the privacy paradox a relic of the past? An in-depth analysis of privacy attitudes and privacy behaviors. *European Journal of Social Psychology*, *45*(3), 285–297. https://doi.org/10.1002/ejsp.2049

Dinev, T., & Hart, P. (2006). An extended privacy calculus model for e-commerce transactions. *Information Systems Research*, *17*(1), 61–80. https://doi.org/10.1287/isre.1060.0080

Dunbar, R. I. M. (1997). Groups, gossip, and the evolution of language. In A. Schmitt, K. Atzwanger, K. Grammer, & K. Schäfer (Eds.), *New aspects of human ethology* (pp. 77–89). Springer. https://doi.org/10.1007/978-0-585-34289-4_5

Edwards, J. R. (2002). Alternatives to difference scores: Polynomial regression analysis and response surface methodology. In F. Drasgow & N. Schmitt (Eds.), *Measuring and analyzing behavior in organizations: Advances in measurement and data analysis* (pp. 350–400). Jossey-Bass.

Edwards, J. R., & Parry, M. E. (1993). On the use of polynomial regression equations as an alternative to difference scores in organizational research. *Academy of Management Journal*, *36*(6), 1577–1613. https://doi.org/10.5465/256822

Faul, F., Erdfelder, E., Buchner, A., & Lang, A.-G. (2009). Statistical power analyses using G*Power 3.1: Tests for correlation and regression analyses. *Behavior Research Methods*, *41*(4), 1149–1160. https://doi.org/10.3758/BRM.41.4.1149

Fogel, J., & Nehmad, E. (2009). Internet social network communities: Risk taking, trust, and privacy concerns. *Computers in Human Behavior*, *25*(1), 153–160. https://doi.org/10.1016/j.chb.2008.08.006

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

Greene, K., Derlega, V. J., & Mathews, A. (2006). Self-disclosure in personal relationships. In A. Vangelisti & D. Perlman (Eds.), *The Cambridge handbook of personal relationships* (pp. 409–427). Cambridge University Press.

Hallam, C., & Zanella, G. (2017). Online self-disclosure: The privacy paradox explained as a temporally discounted balance between concerns and rewards. *Computers in Human Behavior*, *68*, 217–227. https://doi.org/10.1016/j.chb.2016.11.033

Hargittai, E., & Marwick, A. (2016). "What can I really do?" Explaining the privacy paradox with online apathy. *International Journal of Communication*, *10*, 3737–3757. https://ijoc.org/index.php/ijoc/article/view/4655

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

Humberg, S., Dufner, M., Schönbrodt, F. D., Geukes, K., Hutteman, R., van Zalk, M. H. W., Denissen, J. J. A., Nestler, S., & Back, M. D. (2018). Enhanced versus simply positive: A new condition-based regression analysis to disentangle effects of self-enhancement from effects of positivity of self-view. *Journal of Personality and Social Psychology*, *114*(2), 303–322. https://doi.org/10.1037/pspp0000134

Kehr, F., Kowatsch, T., Wentzel, D., & Fleisch, E. (2015). Blissfully ignorant: The effects of general privacy concerns, general institutional trust, and affect in the privacy calculus. *Information Systems Journal*, *25*(6), 607–635. https://doi.org/10.1111/isj.12062

Kezer, M., Sevi, B., Cemalcılar, Z., & Baruh, L. (2016). Age differences in privacy attitudes, literacy and privacy management on Facebook. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace*, *10*(1), Article 2. https://doi.org/10.5817/CP2016-1-2

Kline, R. B. (2015). *Principles and practice of structural equation modeling*. Guilford Publications.

Knijnenburg, B., Raybourn, E., Cherry, D., Wilkinson, D., Sivakumar, S., & Sloan, H. (2017, February 27). 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

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

Lee, H., Park, H., & Kim, J. (2013). Why do people share their context information on social network services? A qualitative study and an experimental study on users' behavior of balancing perceived benefit and risk. *International Journal of Human-Computer Studies*, *71*(9), 862–877. https://doi.org/10.1016/j.ijhcs.2013.01.005

Lutz, C., & Strathoff, P. (2014, April 16). Privacy concerns and online behavior not so paradoxical after all? Viewing the privacy paradox through different theoretical lenses. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.2425132

Masur, P. K. (2019). *Situational privacy and self-disclosure*. Springer. https://doi.org/10.1007/978-3-319-78884-5

Miller, L. C., Berg, J. H., & Archer, R. L. (1983). Openers: Individuals who elicit intimate self-disclosure. *Journal of Personality and Social Psychology*, *44*(6), 1234–1244. https://doi.org/10.1037/0022-3514.44.6.1234

Nestler, S., Humberg, S., & Schönbrodt, F. D. (2019). Response surface analysis with multilevel data: Illustration for the case of congruence hypotheses. *Psychological Methods*, *24*(3), 291–308. https://doi.org/10.1037/met0000199

Nouwens, M., Liccardi, I., Veale, M., Karger, D., & Kagal, L. (2020). Dark patterns after the GDPR: Scraping consent pop-ups and demonstrating their influence. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems* (pp. 1–13). https://doi.org/10.1145/3313831.3376321

Orben, A. C., & Dunbar, R. I. M. (2017). Social media and relationship development: The effect of valence and intimacy of posts. *Computers in Human Behavior, 73*, 489–498. https://doi.org/10.1016/j.chb.2017.04.006

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

Pek, J., Wong, O., & Wong, A. C. M. (2018). How to address non-normality: A taxonomy of approaches, reviewed, and illustrated. *Frontiers in Psychology*, *9*, Article 2104. https://doi.org/10.3389/fpsyg.2018.02104

R Core Team. (2020). *R: A language and environment for statistical computing*. R Foundation for Statistical Computing. https://www.R-project.org/

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

Rousseeuw, P. J., Ruts, I., & Tukey, J. W. (1999). The bagplot: A bivariate boxplot. *The American Statistician*, *53*(4), 382–387. https://doi.org/10.1080/00031305.1999.10474494

Schönbrodt, F. D. (2017). *RSA: An R package for response surface analysis (version 0.9.11)*. https://cran.r-project.org/package=RSA

Shin, W., & Kang, H. (2016). Adolescents' privacy concerns and information disclosure online: The role of parents and the internet. *Computers in Human Behavior*, *54*, 114–123. https://doi.org/10.1016/j.chb.2015.07.062

Simon, H. A. (1955). A behavioral model of rational choice. *The quarterly journal of economics, 69*(1), 99-118. https://doi.org/10.2307/1884852

Stieger, S., Burger, C., Bohn, M., & Voracek, M. (2013). Who commits virtual identity suicide? Differences in privacy concerns, internet addiction, and personality between Facebook users and quitters. *Cyberpsychology, Behavior, and Social Networking, 16*(9), 629-634. https://doi.org/10.1089/cyber.2012.0323

Sundar, S. S., Kang, H., Wu, M., Gu, E., & Zhang, B. (2013). Unlocking the privacy paradox: Do cognitive heuristics hold the key? In S. Bødker, S. Brewster, P. Baudisch, M. Beaudouin-Lafon, & W. E. Mackay (Eds.), *CHI 2013: Changing Perspectives* (pp. 811–816). ACM. https://dl.acm.org/doi/proceedings/10.1145/2470654

Taddicken, M. (2014). The 'privacy paradox' in the social web: The impact of privacy concerns, individual characteristics, and the perceived social relevance on different forms of self-disclosure. *Journal of Computer-Mediated Communication*, *19*(2), 248–273. https://doi.org/10.1111/jcc4.12052

Tamir, D. I., & Mitchell, J. P. (2012). Disclosing information about the self is intrinsically rewarding. In *Proceedings of the National Academy of Sciences* (pp. 8038–8043). PNAS. https://doi.org/10.1073/pnas.1202129109

Trepte, S., Reinecke, L., Ellison, N. B., Quiring, O., Yao, M. Z., & Ziegele, M. (2017). A cross-cultural perspective on the privacy calculus. *Social Media + Society*, *3*(1), 1–13. https://doi.org/10.1177/2056305116688035

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

Waldman, A. E. (2020). Cognitive biases, dark patterns, and the 'privacy paradox'. *Current Opinion in Psychology, 31*, 105–109. https://doi.org/10.1016/j.copsyc.2019.08.025

Wilson, D. W., & Valacich, J. S. (2012). Unpacking the privacy paradox: Irrational decision-making within the privacy calculus. *International Conference on Information Systems, 5*, 4152–4162. https://experts.arizona.edu/en/publications/unpacking-the-privacy-paradox-irrational-decision-making-within-t

Zhang, R., & Fu, J. S. (2020). Privacy management and self-disclosure on social network sites: The moderating effects of stress and gender. *Journal of Computer-Mediated Communication*, *25*(3), 236–251. https://doi.org/10.1093/jcmc/zmaa004

Zhu, M., Wu, C., Huang, S., Zheng, K., Young, S. D., Yan, X., & Yuan, Q. (2021). Privacy paradox in mHealth applications: An integrated elaboration likelihood model incorporating privacy calculus and privacy fatigue. *Telematics and Informatics, 61*, Article 101601. https://doi.org/10.1016/j.tele.2021.101601

About Authors

Murat Kezer (M.A. Koc University) is a doctoral student of psychology at University of Oregon. His research interests include privacy, empathy, interpersonal perception, and moral judgments.

Tobias Dienlin (Ph.D University of Hohenheim) is an assistant professor for Interactive Communication at Department of Communication at University of Vienna. His research interests include social media, privacy, mental health, and open science.

Lemi Baruh (Ph.D University of Pennsylvania) is an associate professor at Koç University Media and Visual Arts Department. His research interests include new media technologies, surveillance, privacy—especially pertaining to attitudes about privacy—and culture of voyeurism.

✉ **Correspondence to**
Murat Kezer, Department of Psychology, University of Oregon, Eugene, OR 97403-1227, USA,
mkezer@uoregon.edu