Understanding the effects of personalization as a privacy calculus: Analyzing self-disclosure across health, news, and commerce contexts

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

DOI
10.1093/jcmc/zmy020

Publication date
2018

Document Version
Final published version

Published in
Journal of Computer-Mediated Communication

Understanding the Effects of Personalization as a Privacy Calculus: Analyzing Self-Disclosure Across Health, News, and Commerce Contexts[†]

Nadine Bol

Amsterdam School of Communication Research/ASCoR, University of Amsterdam, Amsterdam, The Netherlands

Tobias Dienlin

Department of Media Psychology, University of Hohenheim, Stuttgart, Germany

Sanne Kruikemeier

Amsterdam School of Communication Research/ASCoR, University of Amsterdam, Amsterdam, The Netherlands

Marijn Sax

Institute for Information Law/IViR, University of Amsterdam, Amsterdam, The Netherlands

Sophie C. Boerman and Joanna Strycharz

Amsterdam School of Communication Research/ASCoR, University of Amsterdam, Amsterdam, The Netherlands

Natali Helberger

Institute for Information Law/IViR, University of Amsterdam, Amsterdam, The Netherlands

Claes H. de Vreese

Amsterdam School of Communication Research/ASCoR, University of Amsterdam, Amsterdam, The Netherlands

The privacy calculus suggests that online self-disclosure is based on a cost–benefit trade-off. However, although companies progressively collect information to offer tailored services, the effect of both personalization and context-dependency on self-disclosure has remained understudied. Building on the privacy calculus, we hypothesized that benefits, privacy costs, and trust would predict online self-disclosure. Moreover, we analyzed the impact of personalization, investigating whether effects would differ for health, news, and commercial websites. Results from an online experiment using a representative Dutch sample (N = 1,131) supported the privacy calculus,

Corresponding author: Nadine Bol; e-mail: n.bol@uva.nl

[†]This manuscript features online supplementary material (OSM), which includes the data of the study, additional analyses, the script of the analyses, and a reproducible version of the manuscript. The OSM can be accessed here: https://osf.io/bq7nt/?view_only=c1f39ba7fc5d417aab7f6616a11db29c

Editorial Record: First manuscript received on February 02, 2018. Revisions received on July 12, 2018. Accepted by Sonja Utz on August 27, 2018. Final manuscript received on August 31, 2018. First published online on 22 October 2018.

revealing that it was stable across contexts. Personalization decreased trust slightly and benefits marginally. Interestingly, these effects were context-dependent: While personalization affected outcomes in news and commerce contexts, no effects emerged in the health context.

Keywords: Personalization, Privacy Calculus, Perceived Benefits, Perceived Privacy Costs, Trust, Self-Disclosure.

doi:10.1093/jcmc/zmy020

Through partaking in online activities, people are producing large amounts of personal information that is being shared with companies (Acquisti, Brandimarte, & Loewenstein, 2015). Companies, in turn, use this information to tailor online services, offering personalized communications based on individuals' interests, behaviors, and needs. These personalized communications result from a constant loop of user input (in the form of personal data) and system output (in the form of personalized services), and influence people's perceptions and decisions online. Such personalized services present several benefits for consumers, fostering perceived relevance, attention, and elaboration (e.g., Lustria et al., 2016). However, the implicit collection of personal data also poses profound challenges for privacy (Awad & Krishnan, 2006), forcing users to constantly decide whether they want to disclose personal information in future online transactions or not.

Self-disclosure reflects the amount of true information people reveal about themselves (Jourard, 1964), for instance when providing personal details for online purchases. Initially, several studies have demonstrated that perceived risks connected to privacy do not always discourage people from disclosing personal information online (e.g., Taddicken, 2014). This inconsistency of privacy attitudes and privacy behaviors has been referred to as the "privacy paradox" (Barnes, 2006). However, in the meantime, an increasing number of studies have found significant relations between privacy concerns and self-disclosure (e.g., Dienlin & Trepte, 2015). Most recently, a meta-analysis showed that the association between privacy concerns and information sharing was small but significant (Baruh, Secinti, & Cemalcilar, 2017), which substantiates the current conception that people disclose personal information on the basis of a cost–benefit trade-off, the so-called privacy calculus (e.g., Krasnova, Spiekermann, Koroleva, & Hildebrand, 2010).

The privacy calculus offers an explanation as to why the relation between privacy concerns and self-disclosure is small, and why self-disclosure behaviors might not be that paradoxical after all. The calculus posits that both perceived costs and perceived benefits determine whether people are willing to self-disclose: The more benefits people expect, the higher the likelihood of disclosure; the more costs people fear, the lower the likelihood of self-disclosure (Laufer & Wolfe, 1977). We follow a probabilistic understanding of the calculus: Although experiencing costs and benefits affects chances of self-disclosure significantly, it does not follow a deterministic pattern. Behavior remains partially fortuitous, and other factors such as emotions, subjective norms, behavioral control, heuristics, or habits are also likely to influence self-disclosure (e.g., Heirman, Walrave, & Ponnet, 2013). Nonetheless, by considering costs and benefits simultaneously, the privacy calculus could potentially help understand how personalization influences online self-disclosure. As the ever-growing personalization of online services continues to impact user behavior, we still do not know how and under what conditions these effects take place. This article therefore applies the privacy calculus to improve our understanding of the effects of personalization on online self-disclosure, contributing to previous research in three distinct ways.

First, as a basic premise we aim to substantiate and extend the privacy calculus. Although the privacy calculus has been extensively tested in earlier research, most studies have been limited to specific settings, such as social network sites (SNSs) (e.g., Dienlin & Metzger, 2016), location-based apps (Chen, Su, & Quyet, 2017), or virtual health communities (e.g., Kordzadeh, Warren, & Seifi, 2016), often having used only small (e.g., Lee & Kwon, 2015) and/or student samples (e.g., Li, Sarathy, & Xu, 2011). We therefore test the privacy calculus on the basis of a large representative sample of the Dutch population, applying it to several contexts simultaneously. In addition, we strive to extend the privacy calculus by examining which privacy cost is the best predictor of self-disclosure.

Second, although there is already some research on personalization online (e.g., Lee & Lehto, 2010; Taylor, Davis, & Jillapalli, 2009), experimental research testing the effects of personalization on self-disclosure is scarce, with only a few studies adopting such an approach (e.g., Li, 2010). As a result, this study is the first to adopt an experimental approach to test the causal effects of personalization on perceived benefits, perceived costs, trust, and self-disclosure online.

Third, this study aims to elaborate our understanding of the "powerful context-dependence of privacy preferences" (Acquisti et al., 2015, p. 509). Whereas in some situations people place costs before benefits, in others benefits are more important. Cost–benefit trade-offs are dependent on context and assessed based on normative and situational criteria, as well as on previous experience (Acquisti et al., 2015). However, to date we lack systematic knowledge and empirical evidence on exactly how personalization influences cost–benefit trade-offs depending on context. We therefore test how personalization affects the cost–benefit trade-offs in online self-disclosure across three different types of website: health, news, and commerce.

A privacy calculus perspective on understanding self-disclosure

The privacy calculus argues that when users have to decide whether to disclose personal information online, they balance the associated benefits and costs (Laufer & Wolfe, 1977). The most important reason as to why people self-disclose online are the expected benefits (e.g., Krasnova et al., 2010). Expected benefits include, for example, social support, entertainment, tailored information, or monetary rewards. At the same time, the perceived costs of self-disclosing online also play an important role. Specific costs include, for example, identity theft, reputational damage, or loss of control. On a more general level, these costs manifest in more pronounced privacy concerns, privacy risk assessments, or privacy risk beliefs (see RQ1). Recent meta-analyses have confirmed that general costs such as privacy concerns and perceived risk negatively impact self-disclosure, such that when users are concerned about privacy and perceive high privacy risk they are less likely to disclose personal information to online services (Baruh et al., 2017). We therefore expect the following:

H1: People who expect more benefits from self-disclosure online are more willing to self-disclose.

H2: People who expect more privacy costs from self-disclosure online are less willing to self-disclose.

Notwithstanding, the question remains as to which kind of privacy cost is most relevant to self-disclosure online. To date, studies have defined privacy costs as privacy concerns (e.g., Dienlin & Trepte, 2015), privacy risk beliefs (e.g., Malhotra, Kim, & Agarwal, 2004), or perceived privacy risk (e.g., Krasnova et al., 2010). Although all three variables have a considerable theoretical overlap, there are still several differences. Online privacy concerns capture whether people are concerned about the practices of information collection by other websites or users, these concerns are both affective and

cognitive. Privacy risk beliefs measure the conceptions people have with regard to data sharing, such as whether it is safe to share data online. As such, risk beliefs measure people's general perceptions. Privacy risk perceptions are two-dimensional and consist of the *likelihood* people attach to privacy breaches and the *severity* of the privacy breaches. They represent a more cognitive appraisal of privacy risk. Whereas some have focused on the more affective privacy concerns as predictors (Dienlin & Trepte, 2015), others have emphasized that the more cognitive privacy risk perceptions can explain self-disclosure the best (Krasnova et al., 2010). To date, however, we do not know which of the three factors, when analyzed together, predicts self-disclosure the best. As a result, we pose the following research question (RQ):

RQ1: When simultaneously including privacy concerns, privacy risk beliefs, and perceived privacy risk perception, which of the three factors is the strongest predictor of self-disclosure?

Apart from benefits and costs, perceptions of trust are also important in understanding self-disclosure online (Metzger & Flanagin, 2013). Trust can be seen as a function of the amount and type of control people have in relationships; it plays a crucial role in weighing the costs and rewards of engaging in social transactions such as self-disclosure (Metzger, 2004). For example, several studies have shown that when people trust online companies, they are more willing to disclose personal information (e.g., Fletcher & Park, 2017). Not surprisingly, scholars have integrated trust into their privacy calculus models and have demonstrated that trust and online self-disclosure behaviors are positively related (e.g., Krasnova et al., 2010). In line with earlier research, we hypothesize:

H3: People who put more trust in online companies are more willing to self-disclose.

Defining personalization and its impact on the privacy calculus and self-disclosure

How people make complex cost–benefit trade-offs to decide whether they will disclose personal information online may depend on the extent to which the information is personalized. We define personalization as the strategic creation, modification, and adaptation of content and distribution to optimize the fit with personal characteristics, interests, preferences, communication styles, and behaviors. It can be understood as a dynamic process, with the interactive, technological, data-mediated relationship between the sender of a personalized message and its receiver at its heart. Personalization in a more rudimentary form represents directed communication, such as addressing people by their respective names. However, in this study we are more interested in personalization of: (a) content (e.g., personal health advice), and (b) distribution (e.g., finding the right news article for the right reader on the right platform at the right time of the day). As personalization often occurs in the form of personalized advertising, we operationalize personalization in this study via advertisements that are created for an individual using information gathered through the individual's online behaviors (Vesanen, 2007).

Both the proliferation and the perception of personalization have changed in recent years: In earlier phases, due to its mechanical nature and lesser reliance on data, personalization had only limited privacy costs; nowadays, however, with its modern data-driven forms of personalization, the collection and processing of personal data has taken center stage, thereby increasing perceived privacy costs and risks (Aguirre, Mahr, Grewal, Ruyter, & Wetzels, 2015). As a consequence, despite potential benefits, personalization can also increase discomfort, leading to perceptions that are more negative. This phenomenon has been termed the "personalization paradox" (Awad & Krishnan, 2006), which states that personalization has positive *and* negative effects. Personalization fosters both the perceived relevance and usefulness of services but, at the same time, also the vulnerability and privacy concerns of their users (Aguirre et al., 2015), which could be expected to result in both an increase and decrease of self-disclosure when partaking in online activities.

To date, we are aware of only one study that analyzed the effects of personalization with a similar focus: Walrave, Poels, Antheunis, van den Broeck, and van Noort (2017) found that personalization had a positive impact on brand attitude, brand engagement, and the intention to forward an advertisement; however, no evidence was found for the expected moderating effect of privacy concerns. As a potential explanation, the authors suggested that perceived benefits and trust in the advertiser may have overshadowed general privacy concerns (Walrave et al., 2017). In line with this study's argumentation, we hence aim to determine whether both positive (i.e., perceived benefits and trust) and negative factors (i.e., perceived privacy costs) might help explain the potential outcomes of personalization. We therefore propose the following question:

RQ2: Does personalization lead to increased or decreased perceived benefits, perceived privacy costs, trust in online companies, and willingness to self-disclose?

Personalization effects on self-disclosure across different contexts

Privacy behaviors are context-dependent (Acquisti et al., 2015): What is appropriate in one context, might be considered private in another. For example, self-disclosing intimate details about one's body is instrumental to patient–doctor interactions but would be inappropriate during a job interview. With her concept of contextual integrity, Nissenbaum (2010) demonstrated the contextual nature of privacy; accordingly, to determine whether a specific transaction of data violates privacy, one should start by identifying the context within which—or the contexts between—the flow of data takes place. Next, one can determine what values are at stake and which contextual norms and expectations this gives rise to. For example, a transaction of data is understood to be appropriate if it respects the norms and expectations in a given context.

In the context of e-commerce, personalization strategies have been used for some time. Key players include advertisers, advertising networks, and (advertising-financed) platforms, with the consequence that consumers now encounter personalization on a daily basis and may have already become accustomed to it. Although personalized advertising can be more relevant to its recipients, it can also generate general feelings of loss of control over one's own data (Smit, van Noort, & Voorveld, 2014), which in turn influences people's willingness to self-disclose to commercial websites (Dinev & Hart, 2006).

Regarding the context of news, personalization is still an area of considerable experimentation. Most prominently, personalization takes place via the selective distribution of news. Motives for personalization are increasing engagement and time spent on the website, gathering more information for commercial purposes, and increasing advertising revenues (e.g., Anderson, 2011). From the perspective of users, news personalization represents a broad palette of possible benefits, which include getting more relevant news and filtering the abundance of information online. On the other hand, personalization is also associated with negative phenomena such as "filter bubbles," and the external influences on the diversity and depth of news is often subject to criticism (Pariser, 2011). Although research has not yet investigated how users respond to personalized news, we may assume that these associated benefits and costs will be balanced by users in their decision to disclose personal information online.

Turning to the context of health, the differences in utility for users become even more evident. Here, the push for more personalized services is not only driven by advertisers and (commercial) providers of health services, but also by medical experts and governments, who see both individual and societal gains in a move toward a more personalized health care system. For users, the benefits of personalized health services differ from news and commerce contexts. For example, while users of personalized news and commerce may hope for better or more personally relevant offers, the benefits of

using personalized health services can quite literally be a matter of life and death. At the same time, self-disclosing personal health data is particularly sensitive and may have far reaching consequences: For example, insurance companies could increase costs depending on a subject's health status or achievement of fitness goals. This may particularly have consequences for self-disclosure. As was found previously, in the context of health, perceived risks may play a more prominent role in explaining self-disclosure behavior than perceived benefits (Li, Wu, Gao, & Shi, 2016).

Xu, Dinev, Smith, and Hart (2008) demonstrated that the contexts of e-commerce, SNSs, finance, and health care can impact negative privacy cognitions such as concerns or privacy risks differently. However, given the expected context-dependency of privacy behaviors, it seems important to explore the extent to which the effects of personalization on the privacy calculus variables and self-disclosure are also context-specific. Do people weigh costs and benefits differently depending on context, and does personalization affect costs, benefits, and self-disclosure only in specific contexts or is it a general phenomenon? We formulate the following questions:

RQ3: Do different contexts (i.e., health, news, and commerce) moderate the relationships between perceived benefits, perceived privacy costs, and trust in online companies on the one hand, and willingness to self-disclose on the other hand?

RQ4: Do different contexts (i.e., health, news, and commerce) moderate the effects of personalization on perceived benefits, perceived privacy costs, trust in online companies, and willingness to self-disclose?

Methods

Experimental design and procedure

We tested all hypotheses and research questions using a scenario-based online experiment, which is a common approach in the domain of online personalized communication (see Bleier & Eisenbeiss, 2015). Participants were randomly assigned to one of six conditions in a 2 × 3 between-subjects design (personalization: personalized vs. non-personalized; context: health vs. news vs. commerce).

In all scenarios, a short introduction instructed participants to imagine themselves searching for information using a search engine, followed by visiting a context-related website. This website was either a health, news, or commerce website, dependent on the experimental condition. The scenarios talked about the search engine and health, news, or commerce websites in general, without giving them specific names. The scenario described how the participant provided their personal information to the website to receive personally relevant information in return (i.e., health advice, suggestions for news articles, or suggestions for new sunglasses). Afterwards, the scenario continued by saying that the participant closed the website and revisited the search engine a few hours later, where the participant did a context-irrelevant search task (i.e., checking the weather forecast online). In the personalized conditions, the scenario explained that during this second search task, the participant was presented with advertisements related to their previous search task. In the non-personalized conditions, these advertisements were unrelated to the previous search task. All scenarios can be viewed in the online supplementary material.[1]

After reading the scenario, participants were asked to complete survey items on perceived benefits, trust, privacy concerns, privacy risk beliefs, privacy risk perceptions, and willingness for future self-disclosure. The institutional review board of the first author's university granted permission for this study (reference number: 2015-CW-69).

Power analysis and participants

To calculate minimum sample size, we conducted a priori power analyses. We based our power analysis on the smallest effect size of interest (SESOI, Lakens, 2014, p. 706). We argued that all effects equal to or above $|\beta| = .10$ are theoretically relevant and empirical support for our hypotheses. As a consequence, all values below, even when statistically significant, are considered too small to be meaningful. The power analysis showed that a sample size of $N = 1{,}293$ was needed to test our hypotheses with a power of 95% and the usual alpha level of 5% (two-tailed). Given the final sample size of $N = 1{,}131$, the achieved power of this study was 92%, which is comparatively high. Therefore, this study is slightly more likely to miss an existing effect ($\beta = 7.91\%$) than to falsely detect a non-existing effect ($\alpha = 5\%$).

The data were representative of the Dutch population aged 18 years or older. Participants were recruited through CentERdata's LISSPANEL in July and August 2017. CentERdata invited 1,473 members from their panel to participate in an online survey, of which 1,148 took part in the study. A total of 17 cases had to be deleted because of missing data, resulting in a final sample size of $N = 1{,}131$. Participants' age ranged between 18 and 90 years ($M = 56$, $SD = 16$), and 50% were female. Regarding education, 6% reported primary education, 25% preparatory secondary vocational education, 10% higher secondary general education or pre-university education, 22% secondary vocational education, 24% higher vocational education, and 13% university. The net median household income was €2,736 per month (about US$3,234).

Pilot study

A pilot study was carried out among a convenience sample of 78 participants to examine the perceived realism of the experimental scenarios and to develop specific benefit measures. The majority of the pilot participants were female ($n = 55$, 71%), and they averaged 38 years of age ($SD = 13$, range = 23–72). Most participants had completed a higher level of education (i.e., higher vocational education or university, $n = 59$, 76%).

Participants were asked to rate the credibility and likelihood of the events described in the scenario on a 7-point scale. On average, the personalization scenarios were rated as more realistic ($M = 5.71$, 95% CI [5.41, 6.01]) than the non-personalization scenarios ($M = 4.63$, 95% CI [4.30, 4.96]). Furthermore, the scenarios in the commerce context ($M = 5.85$, 95% CI [5.69, 6.01]) were perceived as more realistic than in the health context ($M = 4.83$, 95% CI [4.46, 5.20]) and in the news context ($M = 4.88$, 95% CI [4.57, 5.19]). Together with the fact that perceived realism can impact the effects of scenario-based scripts on outcomes (e.g., Siponen, Vance, & Willison, 2012), we hence decided to include perceived realism as control variable in the main study.

In the personalized conditions ($n = 37$), participants were asked to name potential benefits of online self-disclosure. The pilot data revealed three types of benefits: perceived usefulness, personal relevance, and informativeness. Participants mentioned 11 benefits regarding perceived usefulness, such as finding information more quickly. For personal relevance, another 11 mentions were made, such as how information could be adapted to one's personal situation. There were also eight mentions of benefits related to informativeness, such as receiving new information. These categories of perceived benefits were translated into a perceived benefits scale of online self-disclosure (see measures).

Measures

Participants answered all items on a 7-point scale ranging from 1 = *strongly disagree* to 7 = *strongly agree*. Factor validity was tested via confirmatory factor analyses for each variable separately. In addition, to test discriminant validity and item cross-loadings, we computed an overall model analyzing all variables together. Referring to common fit criteria (e.g., Kline, 2016), all measures showed good model fit and reliability; likewise, the overall model revealed good fit (see Table 1). Several items

Table 1 Descriptives and Factorial Validity of all Measures

	m	sd	p(chisq)	cfi	tli	rmsea	srmr	alpha	omega	avevar
Benefit	3.01	1.35	<.001	.94	.92	.10	.04	.95	.95	.69
Trust	2.59	1.30	.375	1.00	1.00	<.01	.01	.91	.91	.72
Risk perception	5.54	1.20	<.001	.98	.96	.08	.03	.89	.96	.82
Risk belief	5.33	1.14	<.001	.97	.95	.07	.02	.82	.84	.52
Privacy concern	5.25	1.36	.167	1.00	1.00	.02	.01	.94	.94	.77
Self-disclosure	2.23	1.28	<.001	.98	.97	.04	.03	.89	.93	.68
Overall			<.001	.95	.95	.04	.06	.83	.94	.70

Note: alpha = internal consistency (Cronbach's alpha); omega = composite reliability (Raykov's omega); avevar = average variance extracted.

violated the assumption of normal distribution (see Figure 1); therefore, we used maximum likelihood estimation with robust standard errors and a Satorra-Bentler scaled test statistic. All items are listed in the online supplementary material.

Perceived benefits

Perceived benefits assessed how many positive aspects people attributed to disclosing personal information online. As described above, eight items were developed on the basis of both the pilot study and previously used perceived benefits scales (Davis, 1989). One sample item was: "Sharing my personal information with [health/shopping/news] websites helps me find information more quickly."

Privacy concerns

Privacy concerns assessed how strongly people worry about their privacy online, and were measured with five items adopted from Baek and Morimoto (2012). One sample item was "I am concerned that personal information I share through [health/shopping/news] websites can be shared with other companies."

Privacy risk perception

Privacy risk perception was measured as a second-order factor, with: (a) perceived susceptibility to privacy violations, and (b) perceived severity of privacy violations as first-order factors. Susceptibility was assessed with three items adopted from Boerman, Kruikemeier, and Zuiderveen Borgesius (2018), including "I think that [health/shopping/news] websites collect information about my online search behavior." Severity was assessed with three items adopted from Boerman et al. (2018). One example item was "I find it problematic if [health/shopping/news] websites collect information about my online search behavior."

Privacy risk beliefs

Privacy risk beliefs measured the expectation that a high potential for loss was associated with the release of personal information to the website described in the scenario. Privacy risk beliefs were assessed with five items adopted from Malhotra et al. (2004), such as "It is risky to share personal information (such as your name, address, and age) with [health/shopping/news] websites."

Trust

Trusting beliefs reflect the degree to which people believe the website in the scenario is dependable in protecting consumers' personal information, and were measured using four items adopted from

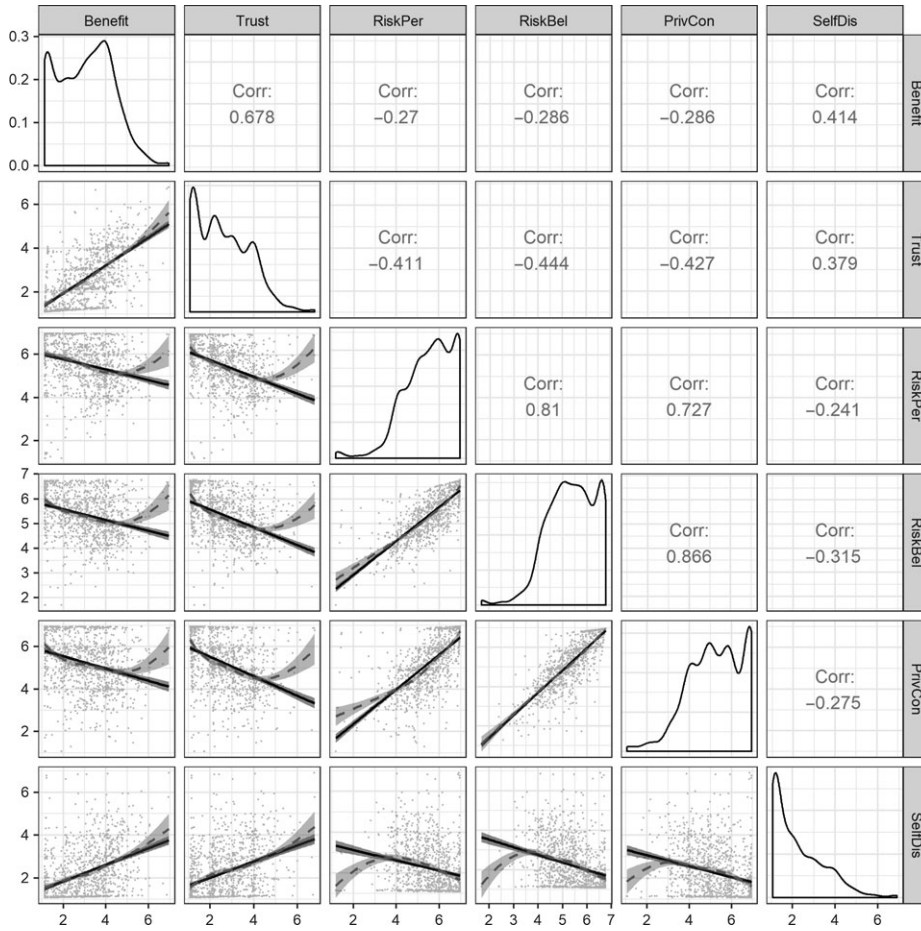

Figure 1 Above diagonal: zero-order correlation matrix; diagonal: density plots for each variable; below diagonal: bivariate scatter plots for zero-order correlations. Solid regression lines represent linear regressions; dotted regression lines represent quadratic regressions. Means were calculated by averaging the predicted values for the indicators of the latent variables.

Malhotra et al. (2004). One example item was: "[health/shopping/news] websites handle my personal information confidentially."

Self-disclosure

Participants were asked to imagine revisiting a similar website as presented in the scenario and to rate their willingness to disclose personal information to this website (e.g., the participant's name, age, ethnicity, or hobbies and interests). The scale was measured as a second-order factor with three subdimensions: (a) personal background (e.g., religious convictions), (b) identity (e.g., name), and (c) socio-economic information (e.g., financial situation).

Additional measures

Perceived personalization was measured with two items from Kalyanaraman and Sundar (2006) on a 7-point scale (1 = *strongly disagree* to 7 = *strongly agree*). First, "The advertisements described in the

scenario are based on my previous online search behavior" and, second, "The advertisements described in the scenario target me as a unique individual." In addition, the scenario's perceived likelihood and credibility was measured with one item each.

Data analyses

In the introduction, all hypotheses and RQs were presented as bivariate relations. It should be noted that we analyzed all variables together in multivariate structural equation models (SEM), thereby controlling for redundancy. To test the hypotheses and research questions, we ran separate models for specific analyses. In all models, we controlled for age, sex, level of education, and the scenario's perceived likelihood and perceived credibility.[2]

For the analyses, coding, and typesetting, we used R (Version 3.5.1; R Core Team, 2018) and the R-packages *ggplot2* (Version 3.0.0; Wickham, 2016), *lavaan* (Version 0.6.3; Rosseel, 2012), *papaja* (Version 0.1.0.9842; Aust & Barth, 2018), *psych* (Version 1.8.4; Revelle, 2018), *pwr* (Version 1.2.2; Champely, 2018), *semTools* (Version 0.5.1; Jorgensen et al., 2018), and *tidyverse* (Version 1.2.1; Wickham, 2017).

All hypotheses were tested using a significance level of 5%. RQ2, because it analyzed the effects of personalization on four different outcomes without specific a priori assumptions, was controlled for alpha error inflation by using a family-wise Bonferroni correction. As a result, the critical alpha for RQ2 was $p{=}\alpha/k = 5\%/4 = 1.25\%$. Likewise, next to the regular 95% confidence intervals, we also report Bonferroni-corrected 98.75% confidence intervals (Figure 2).

With RQ3 and RQ4, we compared three groups: health, news, and commerce. We first tested the SEMs of the respective groups for strict measurement invariance (Kline, 2016, p. 398), which means that both latent factor loadings and item intercepts are equal, with the result that latent factors measure the same construct and can be compared meaningfully across groups. Second, to test RQ3 and RQ4 explicitly, we checked whether the relations between the variables of interest differed for the three groups by conducting structural invariance tests (Kline, 2016). Here, the rationale is that if model fit does not decrease significantly after imposing equality constraints on the structural model (i.e., on the coefficients of the latent variables), the relations between the variables are similar across groups. For all invariance tests, we used Satorra-Bentler scaled chi square difference tests.

The assumption of strict measurement invariance was violated for the three context groups: $\Delta(\chi^2) = 203.84$, $\Delta(p) < .001$. In conclusion, we manually imposed strict measurement invariance for all analyses that compare groups. The final model fit the data well: $\chi^2(332){=}959.86$, $p < .001$, CFI = .97, TLI = .95, RMSEA = .04, SRMR = .04.

Results

Privacy calculus

First, as a robust and conservative estimate, we plotted the bivariate relations for all variables using mean scores (see the supplementary material for results based on latent factor scores). No relation showed an explicitly curvilinear pattern, and all correlation coefficients were consistent with the privacy calculus (see Figure 1).

Next, we tested all hypotheses and research questions in the multivariate model. Regarding H1, we found that perceived benefits significantly predicted participants' willingness to self-disclose, yielding a small- to medium-sized effect, $\beta = .24$, $b = .18$, 95% CI [.12, .24], $z = 5.68$, $p < .001$. Hence, participants who expected more benefits were more likely to disclose, thereby supporting H1.

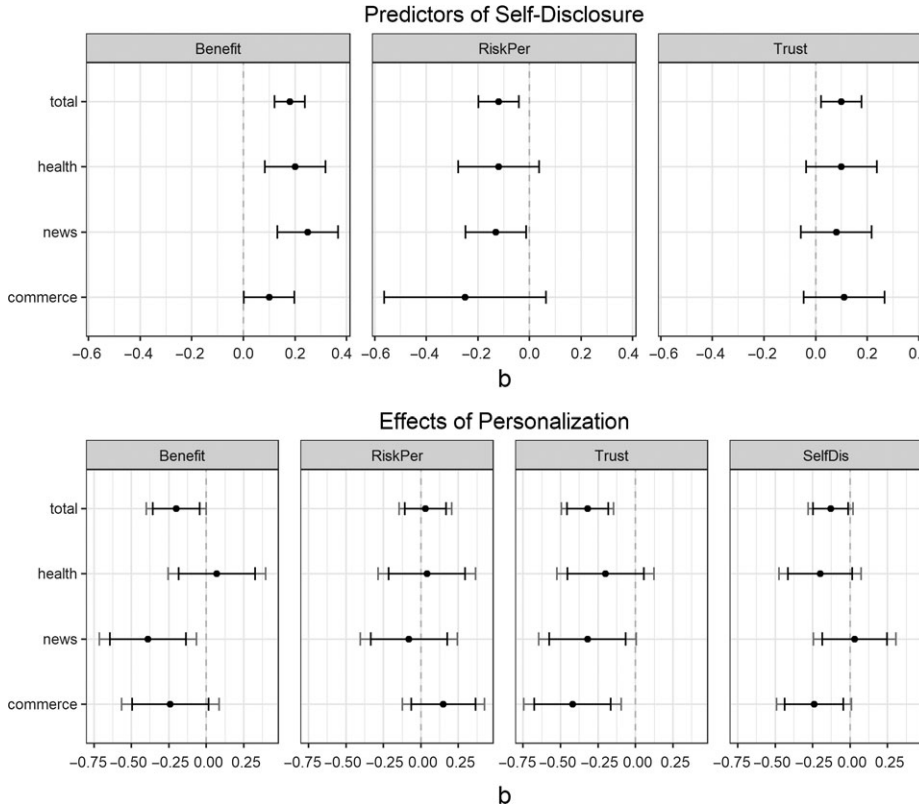

Figure 2 Plots of unstandardized coefficients. Above: 95% confidence intervals, showing that the privacy calculus could be replicated ("total": H1–H3). Model comparisons revealed that the coefficients did not differ significantly across the three contexts; $\Delta(x^2) = 3.54$, $\Delta(p) = .739$, RQ3. Below: 95% and (Bonferroni corrected) 98.80% confidence intervals. Model comparisons revealed that the effect of personalization on the privacy calculus differed slightly across the three contexts; $\Delta(x^2) = 15.57$, $\Delta(p) = .049$, RQ4. All effects were controlled for age, sex, education, perceived likelihood of the scenario, and perceived credibility of the scenario.

RQ1 asked whether privacy concerns, privacy risk perceptions, or privacy risk beliefs would best predict willingness to self-disclose. The bivariate relations all showed comparable medium-sized correlations (Figure 1). When analyzed together in an SEM using multiple regression, a different pattern emerged: Whereas privacy concerns and privacy risk beliefs ceased to be a significant predictor, $\beta = .15$, $b = .11$, 95% CI [−.03, .24], $z = 1.57$, $p = .117$; $\beta = -.02$, $b = -.02$, 95% CI [−.15, .12], $z = -.23$, $p = .820$, privacy risk perception remained a substantial and significant predictor of the participants' willingness to self-disclose, $\beta = -.42$, $b = -.43$, 95% CI [−.73, −.13], $z = -2.79$, $p = .005$. With regard to RQ1, we thus conclude that of all analyzed privacy costs, privacy risk perception was the strongest predictor of willingness to self-disclose.

Likewise, when analyzed alongside the other privacy calculus variables in a multiple regression, privacy risk perceptions remained a significant predictor of the willingness to self-disclose, $\beta = -.13$, $b = -.12$, 95% CI [−.21, −.04], $z = -2.76$, $p = .006$. Participants who perceived their privacy to be more at risk, were slightly less likely to self-disclose, thereby supporting H2.

Concerning H3, we found that participants who put more trust in online companies were also slightly more willing to self-disclose, $\beta = .13$, $b = .10$, 95% CI [.02, .17], $z = 2.49$, $p = .013$, supporting H3.

Personalization

Regarding RQ2, we analyzed the effects of personalization on the privacy calculus. The results showed that when people were confronted with personalized communication, they trusted online companies slightly less, $\beta = -.14$, $b = -.32$, 95% CI [−.47, −.18], $z = -4.35$, $p < .001$. In addition, personalization reduced expected benefits marginally, $\beta = -.08$, $b = -.20$, 95% CI [−.35, −.05], $z = -2.64$, $p = .008$; however, note that the effect was below our pre-defined SESOI of $\beta = .10$, implying that the effect is of minor theoretical relevance. Similarly, personalization reduced willingness to self-disclose marginally, $\beta = -.07$, $b = -.13$, 95% CI [−.24, −.01], $z = -2.07$, $p = .039$; nonetheless, given that both the p-value was above the Bonferroni adjusted critical value of $p = .0125$ and the effect size below the SESOI, the effect is negligible. There was no effect of personalization on privacy risk perception, $\beta = .01$, $b = .03$, 95% CI [−.11, .17], $z = .39$, $p = .696$. For an overview of the groups' means, see Table 2.

Contexts

With RQ3, we analyzed whether the privacy calculus would change depending on context. When comparing the structurally constrained model with the structurally unconstrained model, fit did not decrease significantly, $\Delta(\chi^2) = 3.\ 54$, $\Delta(p) = .\ 739$, implying that the relations of the privacy calculus variables did not differ across the three contexts.

With RQ4, we asked whether the effect of personalization on the privacy calculus would change depending on context. The difference was significant, $\Delta(\chi^2) = 15.\ 57$, $\Delta(p) = .\ 049$, implying that the effects of personalization differed slightly across contexts. However, note that the probability of the data is only marginally below the usual significance level of 5%. Specifically, we found that personalization had no significant effects in the health context: It neither reduced expected benefits, $\beta = .03$, $b = .07$, 95% CI [−.18, .33], $z = .56$, $p = .573$, nor risk perception, $\beta = .02$, $b = .04$, 95% CI [−.21, .28], $z = .31$, $p = .760$, trust, $\beta = -.09$, $b = -.20$, 95% CI [−.45, .05], $z = -1.58$, $p = .114$, or self-disclosure, $\beta = -.11$, $b = -.20$, 95% CI [−.42, .03], $z = -1.73$, $p = .084$.

Taken together, whereas the privacy calculus did not depend on context, the effects of personalization differed significantly. At the same time, the differences between the effects were not particularly pronounced. Finally, also note that group-specific analyses/coefficients are based on subsamples, thereby increasing standard errors and reducing power. For an overview of all coefficients, see Figure 2.

Additional analyses

The control variables had several statistically significant relations with self-disclosure. Participants who were older, male, or more highly educated were slightly less willing to self-disclose ($\bar{\beta}_{age} = -.10$, $\bar{\beta}_{sex} = -.05$, $\bar{\beta}_{edu} = -.06$). Participants who considered the scenario to be more likely were also more willing to self-disclose ($\bar{\beta} = .16$). With one exception (i.e., the effect of personalization on expected benefits), the significance of all coefficients reported above did not depend on the inclusion of control variables.[3]

Finally, we also tested whether respondents consciously detected the personalization. In the personalized conditions, respondents were slightly more likely to agree that advertisements were based on previous online search behavior ($M_{pers} = 5.02$, 95% CI [4.88, 5.16]; $M_{npers} = 4.76$, 95% CI [4.60, 4.92]). However, respondents were not more likely to indicate that advertisements targeted them as 'unique individuals' ($M_{pers} = 3.27$, 95% CI [3.13, 3.41]; $M_{npers} = 3.34$, 95% CI [3.20, 3.48]).

Table 2 Descriptives Means for all Conditions

	Benefit	Trust	RiskPer	RiskBel	PrivCon	SelfDis
Overall mean	3.01	2.59	5.54	5.37	5.25	2.23
Personalization						
Non-personalized	3.03	2.68	5.51	5.35	5.22	2.28
Personalized	3.00	2.49	5.56	5.39	5.29	2.19
Context						
Health	2.98	2.65	5.49	5.39	5.27	2.08
News	2.93	2.53	5.57	5.43	5.32	2.21
Commerce	3.12	2.58	5.54	5.28	5.17	2.41
Personalization and Context						
Non-personalized, health	2.90	2.69	5.45	5.39	5.26	2.17
Non-personalized, news	3.02	2.61	5.62	5.49	5.35	2.12
Non-personalized, commerce	3.17	2.73	5.46	5.17	5.04	2.54
Personalized, health	3.08	2.61	5.53	5.39	5.27	1.97
Personalized, news	2.85	2.46	5.53	5.38	5.30	2.30
Personalized, commerce	3.07	2.43	5.63	5.39	5.30	2.28

Note. Means were calculated by averaging the predicted values for the indicators of the latent variables.

When combined, all variables explained 17% of the variance in willingness to self-disclose. A visualization of all results combined can be found in Figure 3.

Discussion

This study used the privacy calculus to understand how people make cost–benefit trade-offs in personalized media environments across the contexts of health, news, and commerce. Although the privacy calculus has already been applied in earlier studies to explain self-disclosure (e.g., Chen et al., 2017; Dinev & Hart, 2006), it has not yet been adopted to investigate the effects of personalization on self-disclosure across different contexts. Privacy behaviors are considered to be context-dependent (Acquisti et al., 2015), thus examining self-disclosure in different contexts increases our understanding of how people weigh perceived benefits, perceived costs, and trust in online companies to make decisions about online self-disclosure. Moreover, we adopted an experimental approach to make causal inferences between personalization and privacy calculus variables, and we used data from a large representative sample to analyze the generalizability of earlier privacy calculus findings.

The first major finding of this study is that it is possible to replicate prior privacy calculus findings, including when a representative sample of the Dutch population is used. Similar to prior research (e.g., Krasnova et al., 2010), findings showed that self-disclosure is dependent on a trade-off between positive beliefs (i.e., perceived benefits) and negative beliefs (i.e., perceived costs). In addition, we found that trust plays an important role in the calculus: If people trust their online provider more, they are also more likely to self-disclose. Again, perceived benefits were the strongest predictors of self-disclosure, which is consistent with prior research in the context of SNSs (e.g., Dienlin & Metzger, 2016). Our findings also lend support for explaining previous privacy paradoxical behaviors, as potential future privacy risks may be outweighed by immediate gratifications of self-disclosure (Acquisti et al., 2015). Next, we showed that of all cost factors, privacy risk perceptions emerged as the strongest

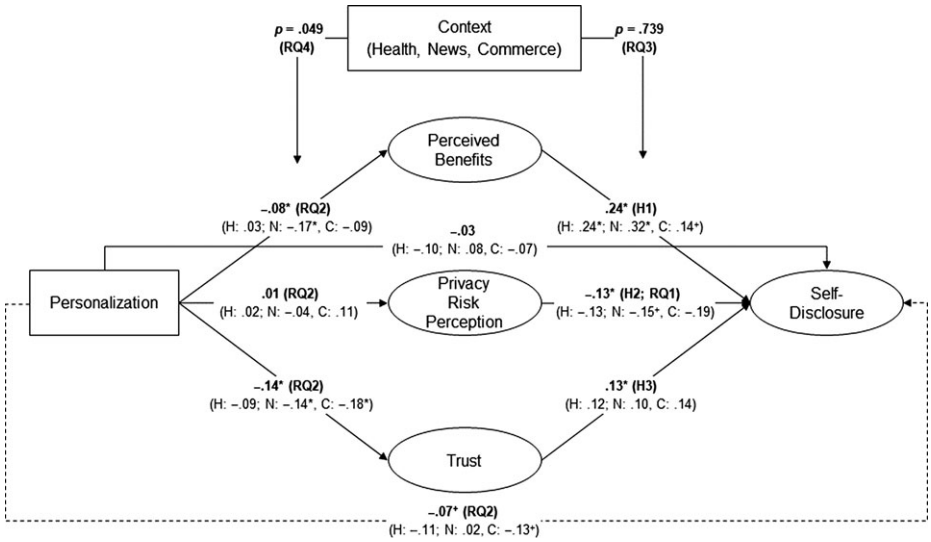

Figure 3 Overview of all results, which combines the analyses from several separate models. Hypotheses 1–3 showed that the privacy calculus could be replicated. RQ1 revealed that, compared to other privacy costs such as privacy concerns or privacy risk beliefs, privacy risk perception was the strongest predictor of self-disclosure. RQ2 showed that personalization reduced trust and, to a small extent, perceived benefits. RQ3 revealed that the privacy calculus variables did not differ across the three contexts. RQ4 showed that the effect of personalization on the privacy calculus differed (slightly) across the three contexts. All effects were controlled for age, sex, education, perceived likelihood of the scenario, and perceived credibility of the scenario. Dotted line represents total effect. H = Health, N = News, C = Commerce. "*" = $p < .05$; "+" = $.05 > p > .0125$ (Bonferroni correction).

predictor of self-disclosure. This finding refutes the position of Dienlin and Metzger (2016), who prioritized privacy concerns, and supports the rationale offered by Krasnova et al. (2010), who focused on risk perceptions. One potential explanation might be methodological: By using a hierarchical second-order measure of risk perceptions, including perceived susceptibility and severity, this study was able to operationalize risk perceptions more broadly and elaborately, thereby potentially improving its predictive capacity. Another tentative explanation might be theoretical: Whereas privacy concerns are more affective and emotional, risk perceptions are more cognitive. So if the process of self-disclosing itself is (partially) rational, it makes sense that risk perceptions also explain more variance. Finally, the results revealed that the privacy calculus pattern emerged similarly in three specific contexts, suggesting that its theoretical pattern is robust and transferable to several contexts.

The second major finding is that through adopting a scenario-based experimental design we were able to test the potential effects of personalization. Results revealed that these effects were mostly negative: Personalization reduced trust and, to some extent, expected benefits as well. In addition, results suggested that personalization may even reduce the willingness for further self-disclosure; however, more research is needed to evaluate whether the effect is substantial and robust. In light of earlier research, our findings are somewhat unexpected. So far, most studies have demonstrated that by increasing both the perceived benefits (e.g., Xu, Luo, Carroll, & Rosson, 2011) and the willingness to self-disclose (e.g., Karwatzki, Dytynko, Trenz, & Veit, 2017) personalization tends to have effects that are positive. As a potential explanation, it is helpful to reconsider the specific framing of our scenarios.

In this study, we first presented the benefits of self-disclosure, considering that participants were told in the scenario that they were able to benefit from specific tailored services after self-disclosing. However, we also presented that afterwards participants received tailored advertisements as a result of self-disclosing online. In doing this, we may have made participants particularly aware of the negative consequences of self-disclosure, which may make these findings different from other research conceptualizing personalization. In prior research, immediate gratifications typically outweighed long-term privacy risks (Acquisti et al., 2015). However, our findings could suggest that personalized advertisements can upend this process by rendering the risks of self-disclosure more salient. In conclusion: While we agree that personalization can have positive effects before and during online transactions, we also contend that it might have negative effects in the long run: Personalization can elucidate risks to privacy—especially if it is used for subsequent advertising. For practitioners, this implies that personalization can also backfire. It seems expedient to protect consumer data and to make sure that subsequent advertisements are not explicitly based on prior self-disclosure, as this might diminish trust and expected benefits.

The third finding is that the effects of personalization can depend on the context in which it is being employed. For instance, although personalization generally led to less trust and decreased perceived benefits, looking more closely at the different contexts revealed that personalization had no significant effects in the health context. As potential explanation, we hypothesize that in health contexts personalization seems to be particularly advantageous, thereby potentially buffering the negative effects we found in the news and commerce contexts. Automatically, it would then become especially important to prevent subsequent personalized advertisements, so as not to reduce trust and willingness for future self-disclosure. However, although the effects of personalization depended significantly on contexts, the overall difference was moderate, so the effects should not be overinterpreted.

With regard to the effect of sociodemographic variables, we for example found that older people and males are less willing to self-disclose, which is in line with prior research (Dienlin & Metzger, 2016). As a result, so as not to overestimate the variables' shared variance, it is important to control for sociodemographic variables when analyzing the privacy calculus.

Limitations and future research

The privacy calculus upholds that disclosure is predominantly rational. Also in this study, the more rational risk perceptions explained more variance than the more affective privacy concerns did. However, online behaviors such as self-disclosure are often automatic, emotional, and situationally dependent (Masur, 2018). For example, past research demonstrated that emotions formed from an impression of a website can impede self-disclosure (Li et al., 2011). In conclusion, although the results showed that self-disclose can be explained partially and probabilistically by rational variables, this still leaves ample room for other influences such as those mentioned. Future research could hence further specify how to account for the "non-rational" aspects of self-disclosure online, such as by investigating other novel factors.

Using a scenario-based approach has several advantages, such as high internal validity. At the same time, this approach also limits ecological validity, which is why we encourage future research to observe and investigate actual behavior online. Nonetheless, scenario-based experiments, such as used for this study, are a commonly used approach in the domain of online personalized communication (e.g., Aguirre et al., 2015; Bleier & Eisenbeiss, 2015), and provide the precise experimental control needed to test the effects and underlying mechanisms of personalization on self-disclosure.

Future research may also focus on further ways to test the context-dependence of personalization effects. To ensure comparability across conditions, we operationalized the contexts of health, news, and commerce in the scenarios such that participants were exposed to advertisements related to

health, news, and commerce. Such operationalizations may not have been sufficiently distinct to detect different levels of perceived benefits, costs, and trust, as receiving personalized advertisements regardless of context can be perceived in similar ways. Hence, although findings showed that the effects of personalization are to some extent context-dependent, future research might differentiate the contexts more clearly by using contexts that are more distinct.

Conclusion

Using a representative sample of the Dutch population, this study adopted an online experiment to test the effects of personalization on the privacy calculus for several contexts. Overall, the results supported the basic assumptions of the privacy calculus, showing that it can be used to explain online behaviors in various contexts. Specifically, results implied that privacy risk perceptions are the strongest cost predictor of online self-disclosure. Personalization can reduce trust in online companies, to some extent expected benefits, and potentially also willingness for future self-disclosure. In contrast to the privacy calculus, the effects of personalization depend on context, emphasizing the need for both practitioners and scholars to investigate how and under what conditions personalization impacts online self-disclosure.

Acknowledgments

The research was funded by and made possible through the University of Amsterdam Research Priority Area 'Personalised Communication' (personalised-communication.net), Principle Investigators Natali Helberger and Claes H. de Vreese.

Notes

1 See https://osf.io/bq7nt/.
2 Control variables should only be included when theoretically relevant. In the context of research on privacy, this assumption is warranted: Age, for example, correlates negatively with self-disclosure and positively with privacy concerns (Dienlin & Metzger, 2016). Next, we are aware that control variables should be measured only before experimental manipulation; given our research design, however, it was not possible to measure perceived likelihood and credibility beforehand, thereby limiting informativeness regarding causality.
3 The online supplementary material includes the results of all control variables on each measure. It also provides the results of the final model without control variables.

References

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

Aguirre, E., Mahr, D., Grewal, D., Ruyter, K. de, & Wetzels, M. (2015). Unraveling the personalization paradox: The effect of information collection and trust-building strategies on online advertisement effectiveness. *Journal of Retailing, 91*(1), 34–49. doi:10.1016/j.jretai.2014.09.005

Anderson, C. W. (2011). Between creative and quantified audiences: Web metrics and changing patterns of newswork in local US newsrooms. *Journalism: Theory, Practice & Criticism, 12*(5), 550–566. doi:10.1177/1464884911402451

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

Awad, N., & Krishnan, M. (2006). The personalization privacy paradox: An empirical evaluation of information transparency and the willingness to be profiled online for personalization. *MIS Quarterly, 30*(1), 13–28. Retrieved from http://www.jstor.org/stable/25148715.

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

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

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

Bleier, A., & Eisenbeiss, M. (2015). The importance of trust for personalized online advertising. *Journal of Retailing, 91*(3), 390–409. doi:10.1016/j.jretai.2015.04.001

Boerman, S. C., Kruikemeier, S., & Zuiderveen Borgesius, F. J. (2018). Exploring motivations for online privacy protection behavior: Insights from panel data. *Communication Research*, *manuscript accepted for publication*.

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

Chen, J. V., Su, B., & Quyet, H. M. (2017). Users' intention to disclose location on location-based social network sites (LBSNS) in mobile environment: Privacy calculus and Big Five. *International Journal of Mobile Communications, 15*(3), 329–353. doi:10.1504/IJMC.2017.083465

Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly, 13*(3), 319. doi:10.2307/249008

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. doi:10.1111/jcc4.12163

Dienlin, T., & Trepte, S. (2015). Is the privacy paradox a relic of the past? An in-depth analysis of privacy attitudes and privacy behaviors. *European Journal of Social Psychology, 45*(3), 285–297. doi: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. doi:10.1287/isre.1060.0080

Fletcher, R., & Park, S. (2017). The impact of trust in the news media on online news consumption and participation. *Digital Journalism, 5*(10), 1281–1299. doi:10.1080/21670811.2017.1279979

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

Jourard, S. M. (1964). *The transparent self*. New York: Van Nostrand.

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

Kalyanaraman, S., & Sundar, S. S. (2006). The psychological appeal of personalized content in web portals: Does customization affect attitudes and behavior? *Journal of Communication, 56*(1), 110–132. doi:10.1111/j.1460-2466.2006.00006.x

Karwatzki, S., Dytynko, O., Trenz, M., & Veit, D. (2017). Beyond the personalization–privacy paradox: Privacy valuation, transparency features, and service personalization. *Journal of Management Information Systems, 34*(2), 369–400. doi:10.1080/07421222.2017.1334467

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

Kordzadeh, N., Warren, J., & Seifi, A. (2016). Antecedents of privacy calculus components in virtual health communities. *International Journal of Information Management, 36*(5), 724–734. doi:10.1016/j.ijinfomgt.2016.04.015

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

Lakens, D. (2014). Performing high-powered studies efficiently with sequential analyses. *European Journal of Social Psychology, 44*(7), 701–710. doi:10.1002/ejsp.2023

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. doi:10.1111/j.1540-4560.1977.tb01880.x

Lee, N., & Kwon, O. (2015). A privacy-aware feature selection method for solving the personalization–privacy paradox in mobile wellness healthcare services. *Expert Systems with Applications, 42*(5), 2764–2771. doi:10.1016/j.eswa.2014.11.031

Lee, J., & Lehto, X. (2010). E-personalization and online privacy features: The case with travel websites. *Journal of Management and Marketing Research, 4*, 1–14.

Li, Y. (2010). Empirical studies on online information privacy concerns: Literature review and an integrative framework. *Communications of the Association for Information Systems, 28*, 453–496. Available at: https://aisel.aisnet.org/cais/vol28/iss1/28

Li, H., Sarathy, R., & Xu, H. (2011). The role of affect and cognition on online consumers' decision to disclose personal information to unfamiliar online vendors. *Decision Support Systems, 51*(3), 434–445. doi:10.1016/j.dss.2011.01.017

Li, H., Wu, J., Gao, Y., & Shi, Y. (2016). Examining individuals' adoption of healthcare wearable devices: An empirical study from privacy calculus perspective. *International Journal of Medical Informatics, 88*, 8–17. doi:10.1016/j.ijmedinf.2015.12.010

Lustria, M. L. A., Cortese, J., Gerend, M. A., Schmitt, K., Kung, Y. M., & McLaughlin, C. (2016). A model of tailoring effects: A randomized controlled trial examining the mechanisms of tailoring in a web-based STD screening intervention. *Health Psychology, 35*(11), 1214–1224. doi:10.1037/hea0000399

Malhotra, N. K., Kim, S. S., & Agarwal, J. (2004). Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model. *Information Systems Research, 15*(4), 336–355. doi:10.1287/isre.1040.0032

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

Metzger, M. J. (2004). Privacy, trust, and disclosure: Exploring barriers to electronic commerce. *Journal of Computer-Mediated Communication, 9*(4), 00. doi:10.1111/j.1083-6101.2004.tb00292.x

Metzger, M. J., & Flanagin, A. J. (2013). Credibility and trust of information in online environments: The use of cognitive heuristics. *Journal of Pragmatics, 59*, 210–220. doi:10.1016/j.pragma.2013.07.012

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

Pariser, E. (2011). *The filter bubble: What the Internet is hiding from you*. New York: Penguin.

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

Revelle, W. (2018). *Psych: Procedures for psychological, psychometric, and personality research*. Evanston, Illinois: Northwestern University. Retrieved from https://CRAN.R-project.org/package=psych

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

Siponen, M., Vance, A., & Willison, R. (2012). New insights into the problem of software piracy: The effects of neutralization, shame, and moral beliefs. *Information & Management, 49*(7–8), 334–341. doi:10.1016/j.im.2012.06.004

Smit, E. G., van Noort, G., & Voorveld, H. A. (2014). Understanding online behavioural advertising: User knowledge, privacy concerns and online coping behaviour in Europe. *Computers in Human Behavior, 32*, 15–22. doi:10.1016/j.chb.2013.11.008

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. doi:10.1111/jcc4.12052

Taylor, D. G., Davis, D. F., & Jillapalli, R. (2009). Privacy concern and online personalization: The moderating effects of information control and compensation. *Electronic Commerce Research, 9*(3), 203–223. doi:10.1007/s10660-009-9036-2

Vesanen, J. (2007). What is personalization? A conceptual framework. *European Journal of Marketing, 41*(5/6), 409–418. doi:10.1108/03090560710737534

Walrave, M., Poels, K., Antheunis, M. L., van den Broeck, E., & van Noort, G. (2017). Like or dislike? Adolescents' responses to personalized social network site advertising. *Journal of Marketing Communications, 5*(1), 1–18. doi:10.1080/13527266.2016.1182938

Wickham, H. (2016). *Ggplot2: Elegant graphics for data analysis*. Springer-Verlag New York. Retrieved from http://ggplot2.org.

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

Xu, H., Dinev, T., Smith, H. J., & Hart, P. (2008). Examining the formation of individual's privacy concerns: Toward an integrative view. ICIS 2008 Proceedings. Retrieved from http://aisel.aisnet.org/icis2008/6.

Xu, H., Luo, X., Carroll, J. M., & Rosson, M. B. (2011). The personalization privacy paradox: An exploratory study of decision making process for location-aware marketing. *Decision Support Systems, 51*(1), 42–52. doi:10.1016/j.dss.2010.11.017