Computers in Human Behavior 77 (2017) 230–239

Contents lists available at ScienceDirect

Computers in Human Behavior

journal homepage: www.elsevier.com/locate/comphumbeh

Full length article

The valuation of privacy premium features for smartphone apps: The influence of defaults and expert recommendations

Leyla Dogruel [a], Sven Joeckel [b, *], Jessica Vitak [c]

[a] Institute of Media and Communication Studies, Freie Universität Berlin, 14195, Berlin, Germany
[b] Seminar of Media and Communication Studies, Universität Erfurt, Nordhäuser Str. 63, 99089, Erfurt, Germany
[c] College of Information Studies, University of Maryland, 4130 Campus Drive, College Park, MD, 20742-4345, USA

ARTICLE INFO

Article history:
Received 7 March 2017
Received in revised form
29 June 2017
Accepted 17 August 2017
Available online 26 August 2017

Keywords:
Mobile apps
Smartphones
Privacy concerns
Privacy preferences
Economics of privacy
Heuristics

ABSTRACT

This study examines the impact of privacy defaults and expert recommendations on smartphone users' willingness to pay for "privacy-enhanced" features on paid applications using a 2 (privacy premium default/no privacy premium default) x 2 (privacy expert recommendation/non-privacy expert recommendation) experimental design. Participants (N = 309) configured four paid apps with respect to privacy features. Selecting premium privacy features was associated with an increased cost, while removing premium privacy features reduced the cost of the application. Replicating findings from behavioral economics on default modes in decision-making, we found that participants presented with apps with privacy premium default features were more likely to retain the more expensive privacy features. However, the recommendation source did not have a significant effect on this relationship. We discuss how these findings extend existing work on users' decision-making process around privacy and suggest potential avenues for nudging users' privacy behaviors on mobile devices.

1. Introduction

With the increasing popularity of mobile applications (apps) on smartphones and tablets (Jung, Kim, & Chan-Olmstedt, 2014), privacy has become a key concern for users as many apps collect and share sensitive user data (Egelman, Porter Felt, & Wagner, 2013). While prior research has demonstrated that consumers express concerns about the treatment of their private information online and that a discrepancy between their attitudes and behaviors can be observed (generally referred to as the "privacy paradox"; Acquisti, Brandimarte, & Loewenstein, 2015), research on consumers' valuation of different privacy options remains limited (Savage & Waldman, 2015).

To unpack how consumers balance privacy considerations with app utility, the present study considers how smartphone users apply economic valuations of privacy when selecting apps to download and use. In a survey, we asked users how much *value* (measured as willingness to pay a monetary premium) they attribute to privacy-protecting features. Using an experimental design, we varied default settings and recommendation source for each app participants rated. Using this approach, we are able to investigate how findings from behavior economics on decision-making (Kahneman, Knetsch, & Thaler, 1991) can be transferred to mobile privacy research. Our design allows us to understand how the presentation of privacy features influences privacy-based decisions. We also evaluate how far we can 'nudge' (Thaler & Sunstein, 2008) consumers toward valuing data privacy more.

Research provides ample empirical evidence suggesting that online users do not actively manage their privacy. Instead, they rely on 'default' modes when it comes to privacy settings on social network sites or smart devices (Stutzman, Gross, & Acquisti, 2012). Taking this finding in combination with research on behavioral nudging—which suggests that defaults are potential interventions in manipulating an individual's choice architecture towards more desirable outcomes (Balebako et al., 2011)—we argue that if privacy protection is set as a default, the valuation of privacy will be higher than situations where privacy protection is not the default. Finally, we test whether the use of 'expert heuristics' enhances consumers' valuation of privacy protection. Together, these analyses provide

* Corresponding author.
E-mail addresses: leyla.dogruel@fu-berlin.de (L. Dogruel), sven.joeckel@uni-erfurt.de (S. Joeckel), jvitak@umd.edu (J. Vitak).

http://dx.doi.org/10.1016/j.chb.2017.08.035
0747-5632/

useful insights to researchers studying privacy and mobile use across new technologies, as well as those designing these tools to encourage privacy-enhancing behaviors.

2. The economics of privacy

2.1. Privacy and smartphone app selection

The concept of privacy describes an individual's ability to control what information he or she wants others to know (Trepte & Reinecke, 2011; Westin, 1967). Privacy can thus be considered a regulatory process whereby individuals determine who should have access to their personal information (Petronio, 2012). Research on managing personal information in the digital age has largely focused on disclosure and self-presentation goals of social media users (Rui & Stefanone, 2013; Vitak, Blasiola, Patil, & Litt, 2015), but also includes use of online applications and services (Popescu & Baruh, 2013). When considering smartphones and privacy, it is not only disclosure of personal information, but also use-related data such as users' location (Lee & Hill, 2013) that increases the importance of managing mobile data privacy. Data transfer and processing by third parties such as app providers create new challenges for smartphone users and for privacy regulation, as such data exchanges often happen without users' awareness.

When browsing apps through iTunes, Google Play, or similar services, users are confronted with many related apps with similar services and functions (Jung, Kim, & Chan-Olmsted, 2014), and they must decide which app best fits their needs based on available information. They may rely on both product information offered by the app (e.g., functions, descriptions) as well as word-of-mouth information by previous consumers (e.g., user reviews, ratings) and recommendation algorithms such as ranks and ratings by the platform itself (Joeckel, Dogruel, & Bowman, 2017).

Recent research has demonstrated that users rarely consider all types of information available to them during the app selection; instead, they rely on a very limited amount of information during the decision-making process. As a result, app selection meets the characteristics of a heuristic decision process (Dogruel, Joeckel, & Bowman, 2015). In this process, privacy information only plays a subordinate role—either ignored or misunderstood (Chin, Felt, Sekar, & Wagner, 2012; Gage Kelley et al., 2012; Porter Felt et al., 2012). For most, this is not due to a lack of concern for or valuing of privacy (Dienlin & Trepte, 2015; Hallam & Zanella, 2017), but is at least partially explained by how current privacy management systems on smartphones operate (Joeckel et al., 2017). Every app includes a list of permissions that grant it access to different mobile functions such as contact data, GPS information, or Internet access. The technical nature of this process causes an information asymmetry between the user—who often has low technical efficacy—and the app provider. According to Acquisti, Taylor, and Wagman (2016), information asymmetries with incomplete information about the actual processing of personal information as well as biases in individual decision making are crucial reasons why users only rarely engage in rational privacy-based decision-making strategies.

From an economic standpoint, the exploitation of user data is part of most app providers' business models, especially when apps are free to use and users instead 'pay' with their data (Beuscart & Mellet, 2008; Dogruel, 2015). As a result, digital and mobile privacy can be evaluated based on the economic value users place on the privacy of their personal information.

2.2. Economics of privacy

Privacy research encompasses approaches from a variety of fields ranging from sociology, psychology, and economics to law (Walther, 2011). We frame the current study through behavioral economics, which has already demonstrated that privacy has an economic valuation (Brandimarte & Acquisti, 2012; Hui & Png, 2006). Behavioral economists argue that, when making decisions about privacy, people exhibit bounded rationality, with privacy decisions being heuristically driven and, therefore, prone to (cognitive) biases (Tversky & Kahneman, 1974). Following this perspective, privacy researchers argue that privacy involves a negotiation between competing tradeoffs (i.e., costs vs. benefits) for the self and others regarding a given piece of information (Acquisti et al., 2016; Hirschprung, Toch, Bolton, & Maimon, 2016). For individuals, both the protection and the revelation of private information are associated with specific costs. For example, individuals may evaluate possible negative effects such as identity theft, but also benefits such as customized product offers or social support when making a disclosure decision (Brandimarte & Acquisti, 2012; Vitak & Ellison, 2013).

Researchers have referred to this tradeoff as privacy calculus (Culnan & Armstrong, 1999; Culnan, 2000). Mediated by trust, internet users weigh privacy concerns against potential benefits (e.g., monetary or related to better service quality, enhanced features). Privacy calculus models have been empirically tested (Dinev & Hart, 2006; Krasnova & Veltri, 2010) and even related to app use (Fife & Orjuela, 2012; Pentina, Zhang, Bata, & Chen, 2016). However, research in behavioral economics highlights that individuals have difficulties effectively identifying risks and benefits and, as a result, are limited in their ability to assign a value to specific information disclosure behaviors (Acquisti & Grossklags, 2012). One reason for these difficulties is that privacy tradeoffs are often inter-temporal. While disclosing personal information may result in immediate benefits (e.g., a discount when purchasing with a customer loyalty card), the associated costs are often more distant in time and uncertain or ambiguous (Acquisti et al., 2016). This is supported by a recent study demonstrating that privacy concerns primarily affect distant-future intentions and have no direct effect on actual behavior (Hallam & Zanella, 2017). As a result, consumer behavior often departs from rational models of consumer behavior when it comes to transactions of personal information and privacy behaviors (Hui & Png, 2006).

Relatedly, monetary incentives and increased convenience in using digital services motivate people to be less concerned about protecting their personal information (Brandimarte & Acquisti, 2012). From an economic standpoint, personal information such as age, gender, or location can be used for targeted advertising or the development of personalized products and prices. Hence, the control of personal information becomes necessary to balance the economic interests between platform or device providers and individual users. Therefore, assigning economic values to different types of information reveals how much the information matters to different people (Acquisti et al., 2016).

Empirical studies on individuals' willingness to pay for privacy have demonstrated that when privacy protection is presented in a more visible way (e.g., through icons), consumers are willing to pay a premium and prefer websites that better protect their privacy (Tsai, Egelman, Cranor, & Acquisti, 2011). On the other hand, a field experiment by Hui, Teo, and Lee (2007) illustrates that monetary incentives have a positive effect on the exchange of information in business transactions. Likewise, Beresford, Kübler, and Preibusch

(2012) found that a discount of one Euro (US$1) toward the purchase of a DVD is a sufficient incentive for students to provide their date of birth and income to an online seller.

Hui and Png (2006) have noted out that differences between one's willingness to accept (WTA) and willingness to pay (WTP) for personal information/privacy helps explain diverging findings related to individual's values of privacy. When asked how much they value specific types of personal information, participants assumed they owned the information. As a consequence, they demanded a higher price in exchange for its (economic) use. When confronted with actual (commercial) interactions, they realized how costly (e.g., if they have to pay a premium) it is to protect their privacy and, as a result, demanded less compensation. These findings help explain why people in "real world" settings accept small incentives.

This seemingly contradictory valuation of privacy in different contexts has been illustrated in a field experiment (Acquisti, John, & Loewenstein, 2013). Consumers could either buy enhanced privacy (getting a $10 gift card instead of $12) or accept intrusion in their privacy (getting a $12 gift card but sharing their personal information). The authors demonstrated that consumers value privacy differently based on how the incentive was presented, i.e., as the amount of money they would accept to disclose private information (WTA) or the amount of money they would have to pay to protect their private information (WTP). Results confirmed that the distribution of privacy valuations differs as expected: People were more willing to accept rewards for disclosing private information than to "invest" money for preventing their purchases being tracked.

In the case of monetary valuations of privacy during app use, a study by Egelman, Porter Felt, and Wagner (2013) assessed whether consumers are willing to pay a premium for enhanced privacy for apps. Results indicated that about a quarter of participants said they would pay a premium price of $1.50 for an app with fewer required permissions, which served as a proxy for enhanced privacy. However, a second experiment showed that when participants could choose between a free-to-use app that included targeted advertising—and, as a result, required more data permissions—and an app that cost $0.99, the vast majority preferred the free-to-use version and accepted the loss of privacy. Using a similar approach, a study by Savage and Waldman (2015) examined users' economic value of privacy in apps based on choice experiments. The authors analyzed participants' WTP for the potential disclosure of different types of information based on the presentation of apps in choice sets. Results indicated that, on average, consumers were willing to pay between $1.19 (location) and $4.05 (contacts) to conceal specific types of information from the app provider.

Taken together, studies examining the economic valuation of data privacy have demonstrated that users value privacy in monetary terms but often to a lesser extent than expected based on the potential risks of sharing personal information with third parties. Users often do not have well-defined preferences on privacy, which makes them prone to context or presentation effects (Acquisti et al., 2015; Hui & Png, 2006). Given this background, our first research question addresses the monetary value of privacy in the app selection process:

RQ1: What is the (relative) value of enhanced privacy in apps for smartphone users?

2.3. The use of defaults as a privacy protection nudge

From a regulatory perceptive, some researchers argue for employing soft paternalism tools such as nudges to guide consumers toward more privacy-sensitive behaviors (Acquisti, 2009). Nudges are subtle changes made in the choice architecture that trigger people's decision-making processes, with the goal to shift behavior toward more desirable outcomes (Thaler & Sunstein, 2008). Nudges typically change the default mode of presenting product alternatives or alter the presentation of product alternatives insofar as desirable options are highlighted (Johnson et al., 2012).

Applying the concept of nudging to smartphone users' awareness of privacy during app selection, a study by Choe, Jung, Lee, and Fisher (2013) demonstrated that including visual indicators (e.g., if an app is more/less privacy intrusive) can help nudge smartphone users away from using more privacy-invasive apps. The successful application of defaults as nudges has already been demonstrated with respect to a broad range of topics (Johnson & Goldstein, 2003; Thaler & Benartzi, 2004). In the case of privacy, a study by Johnson, Bellman, and Lohse (2002) demonstrated that defaults (i.e., opt-out vs. opt-in) are also successful in guiding users toward privacy-enhancement preferences on websites.

Individuals' tendency to adhere to default settings reflects the status quo bias in decision-making research, whereby individuals use the status quo as a reference point and evaluate alternative options as advantageous or disadvantageous to their current situation (Kahneman et al., 1991; Samuelson & Zeckhauser, 1988). Behavioral economists refer to the loss aversion concept, which states that fear of potential losses is more psychologically powerful than pleasure from potential gains. In addition, active choices are more salient in individuals' minds than those not made. As result, individuals experience greater regrets when undesirable consequences follow from action compared to inaction (Korobkin, 1998).

For this study, we examine whether privacy defaults (where individuals do not have to actively select privacy enhancements) represent a feasible method to nudge users toward strong privacy protections on their mobile devices. Based on previous findings regarding consumers' bias to the default options, we expect that:

H1. When privacy-protecting features are set as default, smartphone users are more likely to stick with these features—even when this increases an app's price—compared to low-privacy features being set as default.

2.4. Advocating privacy through expert heuristic

Researchers have demonstrated that heuristics are of relevance when evaluating and selecting information and products in online contexts (Metzger, Flanagin, & Medders, 2010; Sundar & Nass, 2001). For the selection of apps, the recognition heuristic and majority vote heuristic are particularly important to smartphone users' decision making (Burgers, Eden, de Jong, & Buningh, 2016; Joeckel et al., 2017). As underlined in the privacy calculus model (Dinev & Hart, 2006), trust plays a crucial role in online interactions (Culnan & Armstrong, 1999); consequently, the expert/authority heuristic ('experts can be trusted') comes into play as well. Research indicates that experts play a crucial role for evaluating information credibility (Chen & Chaiken, 1999; Metzger et al., 2010). Media users tend to rely on an authority figure they believe provides reliable information or appears trustworthy (Flanagin & Metzger, 2013). This authority may either be a representative (e.g., government source) or is granted credibility based on credentials such as being labeled as an expert (Metzger et al., 2010).

Following the notion that users have difficulties in (rational)

decision making for privacy, we assume that privacy expert recommendations will act as an orientation for users such that they will increase users' preference for privacy-protecting app features. Yet, the mechanism should also work in reverse: Because smartphone users trust privacy experts, this should lead them to follow experts' advice—regardless of what the expert is recommending—as expert heuristics provide a cognitive shortcut that may lead to less cognitive investment by the user. Therefore, in the case of app selection, we predict:

H2. Recommendation by privacy experts moderates the relationship between privacy defaults and WTA/WTP for privacy features such that smartphone users are more likely to follow the default settings.

For analytical purpose, we separate H2 into two specific hypotheses:

H2a. If smartphone users are confronted with a privacy-protecting default recommended by privacy experts, they will be more likely to stick with the default than users not confronted with privacy expert recommendations.

H2b. When privacy experts recommend an app without privacy protection as default, users are more likely to not choose privacy-protecting features compared to those that are not confronted with privacy expert recommendations.

Finally, we consider how the two nudges in this study—default settings and recommender source—interact. While we expect that privacy expert-based recommendations and privacy-by-default settings will result in the highest frequency of selecting privacy-enhancing features, it is not as clear if one of the two nudges will perform better than the other. Therefore, we ask:

RQ2: Which privacy nudge—if either—is more strongly correlated to users' likelihood in selecting enhanced privacy protection for an app?

3. Method

3.1. Participants

We recruited participants through Amazon's Mechanical Turk (MTurk). Potential participants qualified for the study if they were at least 18 years old, owned and regularly used a smartphone, and were a U.S. resident. As compensation, participants received US$1.50 when they completed the questionnaire. A total of $N = 400$ individuals were invited to the study. MTurk samples have proven to be reliable in academic research, yet require special attention with respect to data quality (Huff & Tingley, 2015); therefore we carried out a rigorous review of our dataset. Time to complete the instrument was estimated at 10 min, and internal tests revealed that reading all survey instruction required at least 5 min. We excluded any surveys that were submitted in fewer than 5 min from the start time and manually screened datasets for concerning response patterns. This resulted in a final sample of 309 participants ($M_{age} = 35.04$, $SD = 10.08$, 44% female) used for all analyses. Education level was rather high, with 49% of participants ($n = 152$) having at least one college degree; however, this is consistent with other studies of MTurk workers (Hitlin, 2016).

3.2. Procedure and materials

To address our research questions and hypotheses, we conducted a 2 (privacy as default vs. sharing as default) x 2 (privacy expert vs. non-privacy expert recommendation) +1 (control group) experimental design. We designed four app selection scenarios manipulating the two types of nudges (default settings, recommendation source). In an online survey, participants were presented with four smartphone app overviews, one at a time. These apps included a generic description we created based on existing apps but adjusted to fit the study purpose. The following four apps were selected and introduced with fictitious titles: a) a car sharing app named *Rider*, b) a diabetes app named *My Sugar*, c) a companion and security app named *Home Safe*, and d) a mood adjustment app named *My Mood*. All apps may pose some privacy risks as they share location-based information (*Rider* and *Home Safe*) or personal and health-related information (*My Sugar* and *My Mood*) (Shin & Biocca, 2017). See an example of what participants saw in Fig. 1, Appendix.

Table 1
Overview of experimental groups.

	Recommended by	
	Privacy Experts	Non-Privacy Experts
Premium-Privacy Default	*Experimental group #4*	*Experimental group #3*
Basic-Privacy Default	*Experimental group #2*	*Experimental group #1*

For each app, four sets of features were presented: community support, function, personalization and, as privacy feature, data use. For each of these four features, users could select between two modes ("basic" and "premium"). For example, community support allowed for more (premium) or less (basic) social connectedness. For our privacy manipulation, all premium versions of the data use category highlighted that the user had dedicated ownership of all data, in contrast to the basic version, where data was shared with third parties (for an example, see Fig. 2, Appendix).

All apps were marked with a fixed price of US$0.99. Basic features were free and premium features each cost an additional US$0.50, resulting in prices ranging from US$0.99 (when only basic features were selected) and US$2.99 (when all four premium features selected). The selection of either the basic or premium versions for each attribute leads to a higher/lower total sum for the product. Participants could personalize each app according to their preferences and willingness to pay.

Participants were randomly assigned to either the control group or one of the four experimental groups. In the control group, apps were introduced to participants as well as the types of attributes. Participants were free to select what products features with what value (high/low) they liked to choose. The experimental groups differed with respect to privacy premium features been selected as default or not and with respect to privacy experts or non-privacy experts (e.g. app developer) recommending the app. Table 1 gives an overview of our four experimental groups.

Participants in the four experimental conditions viewed apps with a pre-determined default list of features. Apps were presented in a randomized order. In the high privacy condition, "Data Use" was always set to premium. In the low privacy condition, "Data Use" was always set to basic. The other three features varied systematically with respect to basic or premium feature, with *Rider* having no (other) premium feature set as default, *My Sugar* having one ("Community"), *Home Safe* two ("Community," "Function") and *My Mood* three ("Community," "Function," "Personalization"). After viewing each app's description, participants were asked to evaluate the app. They were then asked to customize the app by changing at least one feature. All features in both variations were presented side by side. Once the change(s) were made, the new price was presented and users were again asked to evaluate the customized version.

In the control condition, participants only viewed each app once, and there were no pre-selected features. They could individually select which features were set as basic and which were premium. This was used as a baseline measure for the individual features valuation. Evaluation of the app took place after it had been customized. After finishing the product choice tasks, participants were asked about their general smartphone use, privacy attitudes, and socio-demographic factors.

3.3. Measures

3.3.1. Preference of privacy premium features selected

As the importance participants attributed to enhanced privacy features could differ across the four tasks and as this preference could be a function of both the app and the user's characteristics, we set out to average out these potential differences in privacy importance. Therefore, we counted how many times a privacy protecting premium feature was selected (or remained selected) for the customized app across all four tasks. Scores could range from 0 to 4.

3.3.2. Willingness to pay/willingness to accept score for premium features

Across all conditions and all four tasks, we calculated how many premium features (each valued at 50 cents) were selected. From this score, we deducted the value of selected privacy premium features and calculated an average score per app. The score could range from 0 to 3 cents.

We also collected data for the following control variables:

Participants' app product preferences. In the control condition, we captured participants' app preferences by coding what app features they selected as basic or premium.

App evaluation. For app evaluation, we relied on a scale inspired by Reichheld (2003) research on the net promoter score. In the experimental conditions, participants were asked to rate how likely they would be to recommend the app as displayed in the default mode to a friend who may need it on 7-point scale (1 = very unlikely to 7 = very likely). After customizing each app, participants in all conditions were asked the same question (control group participants only responded once). Both measures acted as a control to compare the attractiveness of customized app versions across all conditions.[1]

Prior paid app use. We asked participants how many paid apps they had downloaded previously. Scores ranged from 0 (35%, $N = 309$) to 100 ($M = 5.33$, $SD = 11.5$)

Privacy concerns. We assessed respondents' privacy concerns using apps through an adapted version of the Mobile Users' Concerns for Information Privacy (MUIPC) scale (Xu, Rosson, Gupta, & Carroll, 2012). Nine items measured perceived surveillance, perceived intrusion, and secondary use of personal information along a five-point Likert-type scale ranging from 1 = fully disagree to 5 = fully agree ($M = 3.82$, $SD = 0.89$) Internal consistency was high with $\alpha = 0.939$ ($n = 309$).

Socio-demographics. Age, sex, and highest level of educational completed were collected from participants.

[1] Due to a technical glitch in the survey, an incorrect text description was shown for the MySugar app. Therefore, we excluded this app from the analysis of this control variable. Please note that data patterns remain the same if data on this app are included.

4. Results

4.1. Descriptive statistics and randomization check

To investigate the effects of our experimental manipulation on privacy valuations, first we checked if our randomized groups differed significantly with respect to control variables, including socio-demographics. We did not find any significant differences between the groups (four experimental groups as well as control group) for age, $F(4, 304) = 1.23$, $p = 0.30$, gender, $F(4, 300) = 0.52$, $p = 0.72$, education, $F(4, 302) = 0.47$, $p = 0.76$, privacy concerns, $F(4, 304 = 1.86$, $p = 0.12$), or number of paid apps used, $F(4, 303) = 0.92$, $p = 0.45$.[2]

As a second test, we investigated how far the preference for the customized apps differed as a function of default settings (free-to-select, basic privacy as default, premium privacy as default). We used the average evaluation scores across three (*Rider*, *Home Safe*, *My Mood*) of the four apps (see footnote 1). Customized apps in the control condition ($M = 4.26$, $SD = 1.51$, n = 61) were rated more positively than those in the basic privacy feature ($M = 3.96$, $SD = 1.50$, n = 126) and those in the premium privacy feature condition ($M = 4.14$, $SD = 1.49$, n = 122); however, differences between the groups were not significant, $F(2, 306) = 0.93$, $p = 0.40$). We further tested for the experimental factor privacy default (default: basic privacy vs. default: premium privacy) to determine if the customized apps were rated more positively than the default app options. As expected, app evaluation scores for the apps with pre-selected features (basic privacy default: $M = 3.48$, $SD = 1.34$, $n = 126$; premium privacy features: $M = 3.57$, $SD = 1.36$, n = 122) were significantly lower than for the customized version (basic privacy default: $t = -6.44$, $df = 125$, $p < 0.001$; premium feature default: $t = -8.46$, $df = 121$, $p < 0.001$).

4.2. The valuation of privacy premium features (control condition)

To answer RQ1, we focused on our control condition, in which participants were free to select the features they wanted for an app. On average, participants in the control condition selected a privacy premium feature 1.69 times ($SD = 1.46$, $n = 61$) out of four potential times.

The preference for privacy premium features was significantly higher ($t = 5.72$, df = 60, $p < 0.001$) than for a personalization premium feature ($M = 0.74$, $SD = 1.08$, $n = 61$) or a function premium feature ($t = 2.66$, $df = 60$, p = 0.010) ($M = 1.23$, $SD = 1.24$, $n = 61$) but lower ($M = 1.98$, $SD = 1.27$, n = 61) albeit not significantly ($t = -1.61$, $df = 6$, $p = 0.11$) than for a community support premium feature.

4.3. The impact of defaults (H1) and recommendations (H2) on privacy valuations (RQ2)

To test our two hypotheses and RQ2, we carried out two factorial ANCOVAs with our two variables of interest (privacy defaults/recommendations) as factors and the average WTP/WTA privacy premium features as DVs. We controlled for socio-demographics (age, sex, education). Further, we expected that the WTP/WTA for privacy would be affected by two additional factors: first, by privacy

[2] For the sake of this test, we considered education (ranging from 1 = no high school degree to 6 = post graduate education as well as gender coded 1 = male, 2 = female as metric variables. Please note that this is not considered a test of equivalence for all groups but a common procedure to inspect the data for substantial divergences from random distributions; based on our data we did not find any indications that required further inquiries.

Table 2
Descriptive Statistics for Number of Privacy Premium Features selected by Experimental Group.

	Recommended by: Privacy Experts *M* (*SD*)	Recommended by: Non-Privacy Experts *M* (*SD*)
Basic-Privacy Default	1.60 (1.44), $n = 62$	1.89 (1.37), $n = 63$
Premium-Privacy Default	2.40 (1.30) $n = 64$	2.64 (1.30), $n = 53$

The number of Privacy Premium Features Ranged from 0 to 4.

Table 3
ANCOVA statistics WTA/WTP for privacy premium feature by experimental group.

	df	*F* (*p*)	η^2
Modelas	9	8.01 (p < 0.001)	0.237
Intercept	1	0.02 (p = 0.880)	0.000
Age	1	1.26 (p = 0.262)	0.005
Gender	1	0.02 (p = 0.876)	0.000
Education	1	1.07 (p = 0.301)	0.005
#Paid apps	1	5.06 (p = 0.025)	0.021
Privacy Concerns	1	4.34 (p = 0.038)	0.018
WTP/WTA Premium	1	30.12 (p < 0.001)	0.115
Condition: Default	1	22.07 (p < 0.001)	0.087
Condition: Recommendation	1	1.35 (p = 0.247)	0.006
Default*Recommendation	1	0.32 (p = 0.571)	0.001
Error	232		

Adj. $r^2 = 0.207$.

concerns and second by their overall willingness to pay for apps. For the first, we employed our privacy concerns scale as a further covariate. For the second, we added the number of paid apps participants indicated they had used before as well as the overall average WTP/WTA for premium features excluding privacy premium features as covariates. Descriptive findings are presented in Table 2.

As predicted, we identified a significant main effect of the privacy default mode, contributing to 8.7% of explained variance (see Table 3). If privacy premium is set as a default, participants are more likely to stick with it and invest in more privacy-protecting features compared to participants that had to actively select it. This provides support for H1.

Analyzing the data to address H2 is more complicated. Overall, we did not see a significant effect for the recommendation manipulation, and the interaction between our two manipulations was not significant (see Table 3). Looking at the descriptive statistics (Table 2), we do not find any support for H2a. In other words, when privacy premium features are set as default and privacy experts recommend it, participants are not willing to pay more for it and they are not more likely to stick with premium privacy features compared to when an app does not carry that recommendation. On the other hand, we see some weak and non-significant support for H2b. When privacy experts recommended an app without privacy premium features, participants were less willing to pay for a privacy premium feature compared to participants who had not received an expert recommendation. Overall, we do not have sufficient evidence to support either H2a or H2b.

With respect to our covariates, we found three additional significant predictors for users' WTA/WTP for privacy features: (1) the overall willingness to pay for premium features, which is responsible for the biggest part of explained variance in our model, (2) the number of paid apps previously installed, and (3) participants' mobile-based privacy concerns. Thus, the more one is willing to pay for apps, the more paid apps she has already installed, and the greater her privacy concerns, the more likely she is to pay for or accept privacy premium features.

As a final step, we compared all five groups (i.e., the four experimental groups and the control group) with respect to the WTP/WTA for privacy features in a one-way ANOVA. This analysis revealed significant differences between the groups, $F(4, 304) = 6.10$, $p < 0.001$). Based on a Duncan post-hoc test, we can derive two homogenous subsets ($p < 0.05$ level). One subset is comprised of the control condition and the two groups with non-privacy defaults, while the second subset contains the two groups with privacy premiums features as default. With respect to RQ2, we conclude that the privacy premium default alone, regardless of expert recommendations, significantly increases participants' WTP/WTA for privacy premium features beyond what they would choose if no default was set.

5. Discussion

In this paper, we explored how much smartphone users are willing to pay for privacy-protecting features—and how this willingness compared with willingness to pay for other common app features. Our analysis found that smartphone users confronted with default privacy premium features at a (virtual) cost of US$0.50 were more willing to accept the indicated price instead of experiencing a loss in privacy when deselecting this premium feature. This happened roughly in 1.7 out of four cases during our app customization tasks. In comparison to other premium features, privacy premium features were the most favorable options for app customization, together with community support features. In line with previous findings on both users' limited WTP for privacy in online contexts as well as the discrepancy between WTP and WTA for the case of privacy (Acquisti et al., 2013; Hui & Png, 2006), our findings support the notion that participants' overall WTP for privacy is lower than their WTA.

Additionally, we examined in how far expert recommendations—together with privacy defaults—may guide users toward a higher valuation of privacy. We found privacy expert recommendations acted as a double-edged sword. In our empirical data, we did not see any benefit derived from using privacy expert recommendations to nudge users' behavior to greater privacy protections—at least when compared to more generic recommendations. There are several possible explanations for why the data trended in this manner. For example, researchers have found that when consumers are making purchasing decisions, they often rely on surface-level signals to support their decision (Häubl & Trifts, 2000). Likewise, Smith, Menon, and Sivakumar (2005) found that consumers' decision-making process was positively influenced by the presence of reviews, regardless of other contextual factors such as information about the reviewer or content of the review. In the case of this study, participants may have been

more focused on selecting app features and made judgments based solely on the presence of a recommendation rather than the *source* of the recommendation.

At the same time, we see some weak indications to support a contradictory explanation, i.e., that distinctions do exist based on the agent making a recommendation for specific features. The presence of expert recommendations may have decreased the likelihood that users selected or kept privacy protecting premium features. Even though the observed effects were not significant, future research should address this finding further and investigate this potentially negative way privacy expert recommendations might work. One way to interpret this result is as an unintended consequence of individuals' reliance on heuristics, insofar that the cognitive shortcut "experts can be trusted" resulted in a reduced selection of privacy-enhancing features.

On a more general level, our findings suggest that users' willingness to pay is influenced by further variables that impact the likelihood of selecting privacy premium features for apps. Therefore, we argue that users' WTP for privacy is not so much a function of socio-demographic factors, but is based on their overall willingness to pay for apps, coupled with their concerns for mobile privacy.

Taken together, our findings provide important theoretical and practical contributions. Our findings support recent theorizing in nudging research (see Thaler & Sunstein, 2008). Defaults have been found as rather strong nudges to change people's behavior (Sunstein, 2017). This is not only true for privacy settings in general (Stutzman et al., 2012; Noain-Sánchez, 2016) but, based on our study, defaults also work with respect to mobile privacy settings, where privacy-related consequences of selection processes often happen at a subconscious level (Joeckel et al., 2017). Yet, with respect to policymaking, the use of defaults as nudges is controversial and depends on a case-specific cost-and-benefit analysis (Sunstein, 2017). From policymakers' point of view, privacy premium defaults may become a welcome solution to inform users of potential privacy risks in applications (Noain-Sánchez, 2016). That said, as users' overall WTP for apps was found to be one of the strongest predictors for the WTP/WTA privacy premium features, costly privacy defaults may only work for those already willing to pay for apps.

For app developers, our findings are encouraging in so much as privacy protection is valued more by consumers than personalization or content related features. Thus, paid apps that protect users' privacy may have an edge over other paid apps that focus more on other features. The findings from this study provide additional encouragement for app developers to provide more privacy protection as a default in their app offerings.

5.1. Limitations

Several limitations need to be addressed. In our study, we employed an app configurator task. We relied on a sample of U.S.-based participants recruited through Amazon MTurk. Such samples are not representative for the larger (U.S.) population, yet they provide some variance with respect to socio-demographics particularly age, sex, and education (Huff & Tingley, 2015). Even if our experimental manipulation does not require any form of representative sample, we have to be cautious with the generalizability of our findings. More importantly, participants could configure each app according to their needs. In the app marketplace, smartphone users are usually confronted with ready-made apps, sometimes offered as a basic, free version and a paid premium version. Thus, the tasks may have been perceived as artificial, which could have affected participants' privacy valuations. Furthermore, participants never had to invest their own money; rather, they were just configuring apps for other users. As a safeguard, we not only made them configure the app but also included the app evaluation score as an approximation for an app's attractiveness. Based on our findings, we can state that the apps our participants configured were sufficiently attractive.

Similar to other studies in this area (e.g., Egelman, Felt, & Wagner, 2013), we can only make statements for paid apps. Most available apps (Jung et al., 2014) are free and likely entail a different valuation of privacy tradeoffs. Still, we see that WTP for privacy is lower than users' WTA privacy premiums. When premium apps compete with free apps in the marketplace, this automatically puts them in a bad position, as users will not invest as much into privacy protection as they would when only a premium version is available. Likewise, as we employed a specific way to present WTA/WTP (a 50-cent premium for privacy protection), the average scores for WTA/WTP presented here should not be interpreted in concrete monetary terms—they only hold true in relative terms.

We averaged out the scores of four different apps. We did this to account for potential differences in the WTA/WTP for certain apps based on their inherent characteristics. Averaging them out seems a preferable option to better understand the broad picture of privacy valuation. Still, our findings might be overshadowed by biases based on an app's individual characteristic. Even if we did not see a pattern in our data that evaluations for one app substantially differed from the others, we still need to be cautious with the generalizability of our findings. Future research is advised to account for these limitations by moving beyond the laboratory setting of our research and conduct more fieldwork, where we might observe users' willingness to pay for privacy protecting features. As of now, we need to rely on partnering with app developers and commercial enterprises for such an endeavor.

6. Conclusion

Inspiring smartphone users to engage in the often time-consuming practices related to establishing enhanced privacy protections for their personal information is challenging. In what we view as encouraging news for privacy scholars, the present study found that, compared to other app features, options around privacy are highly valued by users. Privacy premium defaults may act as an easy-to-administer and effective mechanism to nudge users towards more privacy-sensitive choices. Overall, our research suggests that smartphone users' WTA premiums for privacy protecting features is substantially higher than their WTP for it. Future researchers should continue to explore ways to nudge users to protect their personal information when downloading apps to better fulfill their personal needs.

Appendix

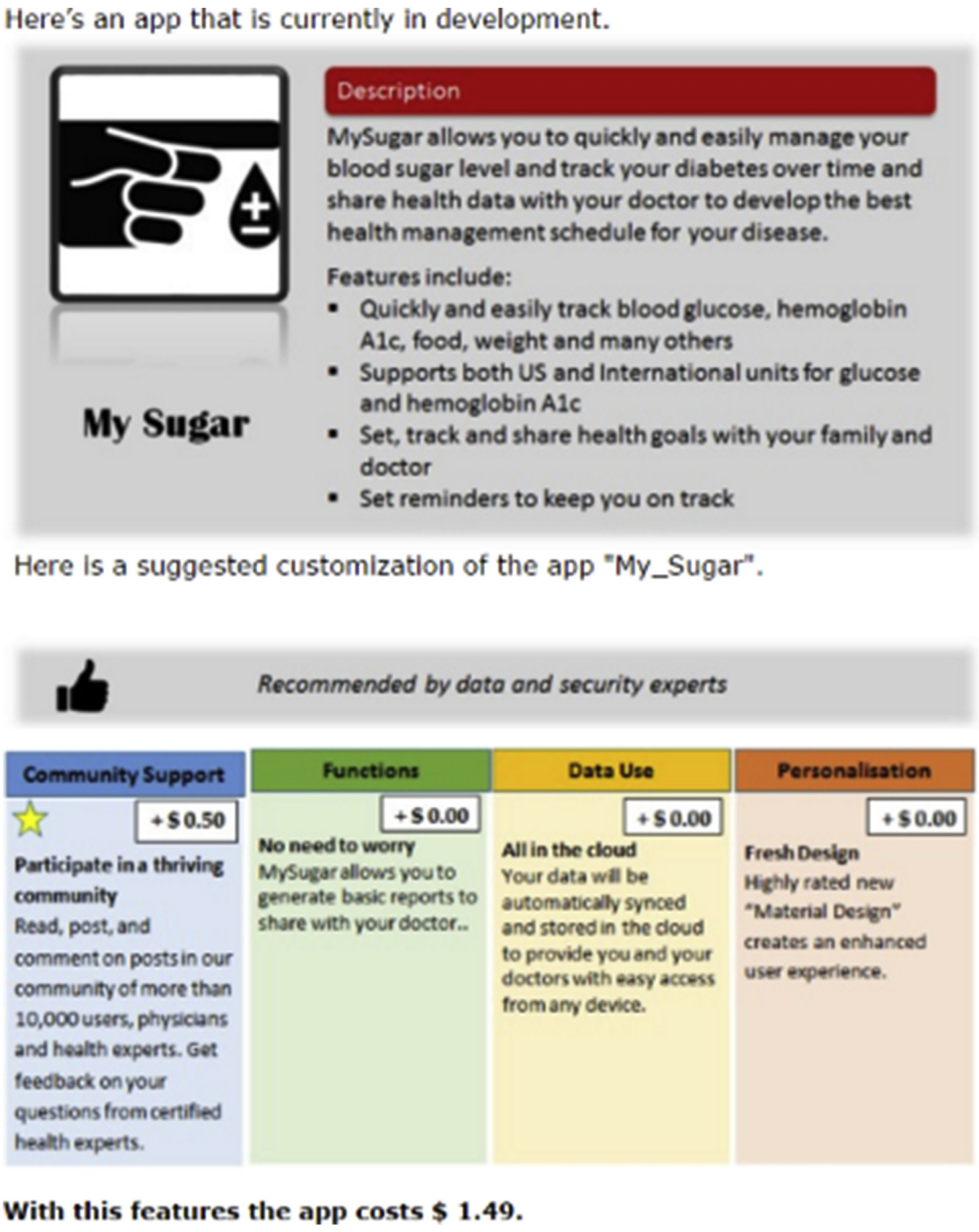

Fig. 1. Example for the app Configuration task.

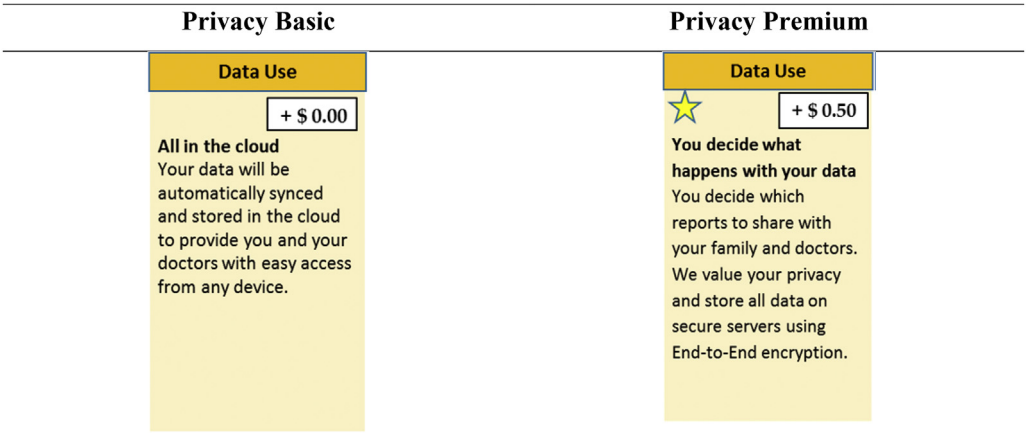

Fig. 2. Privacy Premium vs. Privacy Basic Features – Example My Sugar.

References

Acquisti, A. (2009). Nudging Privacy: The behavioral economics of personal information. *IEEE Security & Privacy Magazine, 7*(6), 82–85. http://dx.doi.org/10.1109/MSP.2009.163.

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

Acquisti, A., & Grossklags, J. (2012). An online survey experiment on ambiguity and privacy. *Communications & Strategies, 88*(4), 19–39.

Acquisti, A., John, L. K., & Loewenstein, G. (2013). What is pivacy worth? *The Journal of Legal Studies, 42*(2), 249–274. http://dx.doi.org/10.1086/671754.

Acquisti, A., Taylor, C., & Wagman, L. (2016). The economics of privacy. *Journal of Economic Literature, 54*(2), 442–492. http://dx.doi.org/10.1257/jel.54.2.442.

Balebako, R., Leon, P. G. L., Almuhimedi, H., Gage Kelley, P., Mugan, J., & Acquisti, A. (2011). Nudging users towards privacy on mobile devices. In *Proc. CHI 2011 workshop on persuasion, nudge, influence and coercion*.

Beresford, A. R., Kübler, D., & Preibusch, S. (2012). Unwillingness to pay for privacy: A field experiment. *Economics Letters, 117*(1), 25–27. http://dx.doi.org/10.1016/j.econlet.2012.04.077.

Beuscart, J.-S., & Mellet, K. (2008). Business models of the web 2.0: Advertising or the tale of two stories. *Communications & Strategies*, (Special Issue Nov), 165–181.

Brandimarte, L., & Acquisti, A. (2012). The economics of privacy. In M. Peitz, & J. Waldfogel (Eds.), *The Oxford handbook of the digital economy (pp. o.S)*. Oxford: Oxford Univ. Press.

Burgers, C., Eden, A., de Jong, R., & Buningh, S. (2016). Rousing reviews and instigative images: The impact of online reviews and visual design characteristics on app downloads. *Mobile Media & Communication, 4*(3), 327–346. http://dx.doi.org/10.1177/2050157916639348.

Chen, S., & Chaiken, S. (1999). The heuristic-systematic model in its broader context. In S. Chaiken, & Y. Trope (Eds.), *Dual-process theories in social psychology* (pp. 73–96). New York, NY: Guilford Press.

Chin, E., Felt, A. P., Sekar, V., & Wagner, D. (2012). Measuring user confidence in smartphone security and privacy. In L. F. Cranor (Ed.), *Proceedings of the eighth symposium on usable privacy and security*. New York, NY: ACM (p. 1–1).

Choe, E. K., Jung, J., Lee, B., & Fisher, K. (2013). Nudging people away from privacy-invasive mobile apps through visual framing. In P. Kotzé (Ed.), *Lecture notes in computer science: Vol. 8119. Human-computer interaction* (pp. 74–91). Heidelberg: Springer.

Culnan, M. J. (2000). Protecting privacy online: Is self-regulation working? *Journal of Public Policy & Marketing, 19*(1), 20–26. http://dx.doi.org/10.1509/jppm.19.1.20.16944.

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

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. http://dx.doi.org/10.1287/isre.1060.0080.

Dogruel, L. (2015). Trade-offs between user's privacy and monetarization of SNS: An exploratory perspective on facebook users. *Journal of Social Media Studies, 2*(1), 27–38. http://dx.doi.org/10.15340/2147336621862.

Dogruel, L., Joeckel, S., & Bowman, N. D. (2015). Choosing the right app: An exploratory perspective on heuristic decision processes for smartphone app selection. *Mobile Media & Communication, 3*(1), 125–144. http://dx.doi.org/10.1177/2050157914557509.

Egelman, S., Felt, A. P., & Wagner, D. (2013). Choice architecture and smartphone privacy: There's a price for that. In R. Böhme (Ed.), *The economics of information security and privacy* (pp. 211–236). Berlin, Heidelberg: Springer (Berlin Heidelberg; Imprint; Springer).

Fife, E., & Orjuela, J. (2012). The privacy calculus: Mobile apps and user perceptions of privacy and security. *International Journal of Engineering Business Management, 1*. http://dx.doi.org/10.5772/51645.

Flanagin, A. J., & Metzger, M. J. (2013). Trusting expert- versus user-generated ratings online: The role of information volume, valence, and consumer characteristics. *Computers in Human Behavior, 29*(4), 1626–1634. http://dx.doi.org/10.1016/j.chb.2013.02.001.

Gage Kelley, P., Consolvo, S., Cranor, L., Jung, J., Sadeh, N., & Wetherall, D. (2012). A conundrum of permissions: Installing applications on an android smartphone. In J. Blythe, S. Dietrich, & L. J. Camp (Eds.), *Financial cryptography and data security* (Vol. 7398, pp. 68–79). Heidelberg, Germany: Springer.

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.

Häubl, G., & Trifts, V. (2000). Consumer decision making in online environments: The effects of interactive decision aids. *Marketing Science, 1*, 4–21. http://dx.doi.org/10.1287/mksc.19.1.4.15178.

Hirschprung, R., Toch, E., Bolton, F., & Maimon, O. (2016). A methodology for estimating the value of privacy in information disclosure systems. *Computers in Human Behavior, 61*, 443–453. https://doi.org/10.1016/j.chb.2016.03.033.

Hitlin, P. (2016). *Research in the crowdsourcing age, a case study*. Washington, DC: Pew Internet Project.

Huff, C., & Tingley, D. (2015). "Who are these people?": Evaluating the demographic characteristics and political preferences of MTurk survey respondents. *Research & Politics, 2*(3), 205316801560464 https://doi.org/10.1177/2053168015604648.

Hui, K.-L., & Png, I. (2006). The economics of privacy. In T. Hendershott (Ed.), *Handbooks in information systems: V. 1. Economics and information systems* (1st ed., pp. 471–498). Amsterdam, Boston: Elsevier.

Hui, K. L., Teo, H. H., & Lee, S.-Y. T. (2007). The value of privacy assurance: An exploratory field experiment. *MIS Quarterly, 31*(1), 19–33.

Joeckel, S., Dogruel, L., & Bowman, N. D. (2017). The reliance on recognition and majority vote heuristics over privacy concerns when selecting smartphone apps among German and US consumers. *Information, Communication & Society, 20*(4), 621–636. http://dx.doi.org/10.1080/1369118X.2016.1202299.

Johnson, E. J., Bellman, S., & Lohse, G. L. (2002). Defaults, framing and privacy: Why opting in-opting out. *Marketing Letters, 13*(1), 5–15. http://dx.doi.org/10.1023/A:1015044207315.

Johnson, E. J., & Goldstein, D. (2003). MEDICINE: Do defaults save lives? *Science, 302*(5649), 1338–1339. http://dx.doi.org/10.1126/science.1091721.

Johnson, E. J., Shu, S. B., Dellaert, B. G. C., Fox, C., Goldstein, D. G., & Häubl, G. (2012). Beyond nudges: Tools of a choice architecture. *Marketing Letters, 23*(2), 487–504. http://dx.doi.org/10.1007/s11002-012-9186-1.

Jung, J., Kim, Y., & Chan-Olmsted, S. (2014). Measuring usage concentration of smartphone applications: Selective repertoire in a marketplace of choices. *Mobile Media & Communication, 2*(3), 352–368. http://dx.doi.org/10.1177/2050157914542172.

Kahneman, D., Knetsch, J. L., & Thaler, R. H. (1991). Anomalies: The endowment effect, loss aversion, and status quo bias. *Journal of Economic Perspectives, 5*(1), 193–206. http://dx.doi.org/10.1257/jep.5.1.193.

Korobkin, R. (1998). The status quo bias and contract default rules. *Cornell Law Review, 83*, 608–687.

Krasnova, H., & Veltri, N. F. (2010). Privacy calculus on social networking sites: Explorative evidence from Germany and USA. In *System sciences (HICSS), 2010 43rd Hawaii international conference on* (pp. 1–10). Chicago: IEEE. http://dx.doi.org/10.1109/HICSS.2010.307.

Lee, H. H., & Hill, J. T. (2013). Moderating effect of privacy self-efficacy on location-based mobile marketing. *International Journal of Mobile Communications, 11*(4), 330. http://dx.doi.org/10.1504/IJMC.2013.055747.

Metzger, M. J., Flanagin, A. J., & Medders, R. B. (2010). Social and heuristic approaches to credibility evaluation online. *Journal of Communication, 60*(3), 413–439. http://dx.doi.org/10.1111/j.1460-2466.2010.01488.x.

Noain-Sánchez, A. (2016). "Privacy by default" and active "informed consent" by layers: Essential measures to protect ICT users' privacy. *Journal of Information, Communication and Ethics in Society, 14*(2), 124–138. http://dx.doi.org/10.1108/JICES-10-2014-0040.

Pentina, I., Zhang, L., Bata, H., & Chen, Y. (2016). Exploring privacy paradox in information-sensitive mobile app adoption: A cross-cultural comparison. *Computers in Human Behavior, 65*, 409–419. https://doi.org/10.1016/j.chb.2016.09.005.

Petronio, S. (2012). *Boundaries of privacy: Dialectics of disclosure*. Albany,NY: State University of New York Press.

Popescu, M., & Baruh, L. (2013). Captive but mobile: Privacy concerns and remedies for the mobile environment. *The Information Society, 29*(5), 272–286. http://dx.doi.org/10.1080/01972243.2013.825358.

Porter Felt, A., Hay, E., Egelman, S., Haneyy, A., Chin, E., & Wagner, D. (2012). Android permissions: User attention, comprehension, and behavior. In *SOUPS '12 proceedings of the eighth symposium on usable privacy and security (article No. 3)*. New York, NY: ACM. Retrieved from http://www.guanotronic.com/~serge/papers/soups12-android.pdf.

Reichheld, F. (2003). The one number you need to grow. *Harvard Business Review, 81*(12), 46–54.

Rui, J. R., & Stefanone, M. A. (2013). Strategic image management online: Self-presentation, self-esteem and social network perspectives. *Information, Communication & Society, 16*(8), 1286–1305. http://dx.doi.org/10.1080/1369118X.2013.763834.

Samuelson, W., & Zeckhauser, R. (1988). Status quo bias in decision making. *Journal of Risk and Uncertainty, 1*(1), 7–59. http://dx.doi.org/10.1007/BF00055564.

Savage, S. J., & Waldman, D. M. (2015). Privacy tradeoffs in smartphone applications. *Economics Letters, 137*, 171–175. http://dx.doi.org/10.1016/j.econlet.2015.10.016.

Shin, D.-H., & Biocca, F. (2017). Health experience model of personal informatics: The case of a quantified self. *Computers in Human Behavior, 69*, 62–74. https://doi.org/10.1016/j.chb.2016.12.019.

Smith, D., Menon, S., & Sivakumar, K. (2005). Online peer and editorial recommendations, trust, and choice in virtual markets. *Journal of Interactive Marketing, 19*, 15–37. http://dx.doi.org/10.1002/dir.20041.

Stutzman, F., Gross, R., & Acquisti, A. (2012). Silent listeners: The evolution of privacy and disclosure on facebook. *Journal of Privacy and Confidentiality, 4*(2), 7–41.

Sundar, S. S., & Nass, C. (2001). Conceptualizing sources in online news. *Journal of Communication, 51*(1), 52–72. http://dx.doi.org/10.1111/j.1460-2466.2001.tb02872.x.

Sunstein, C. R. (2017). *Default rules are better than active choosing (often). Trends in cognitive sciences*. Advance online Publication. http://dx.doi.org/10.1016/j.tics.2017.05.003.

Thaler, R. H., & Benartzi, S. (2004). Save more tomorrow™: Using behavioral economics to increase employee saving. *Journal of Political Economy, 112*(S1), S164–S187. http://dx.doi.org/10.1086/380085.

Thaler, R. H., & Sunstein, C. R. (2008). *Nudge: Improving decisions about health, wealth, and happiness*. New York: Penguin Books.

Trepte, S., & Reinecke, L. (2011). The social web as a shelter for privacy and authentic living. In S. Trepte, & L. Reinecke (Eds.), *Privacy online. Perspectives on privacy and self-disclosure in the social web* (pp. 61–74). Heidelberg, New York: Springer.

Tsai, J. Y., Egelman, S., Cranor, L., & Acquisti, A. (2011). The effect of online privacy information on purchasing behavior: An experimental study. *Information Systems Research, 22*(2), 254–268. http://dx.doi.org/10.1287/isre.1090.0260.

Tversky, A., & Kahneman, D. (1974). Judgment under uncertainty: Heuristics and biases. *Science (New York, N.Y.), 185*(4157), 1124–1131. http://dx.doi.org/10.1126/science.185.4157.1124.

Vitak, J., Blasiola, S., Patil, S., & Litt, E. (2015). Balancing audience and privacy tensions on social network sites. *International Journal of Communication, 9*, 1485–1504, 1932–8036/20150005.

Vitak, J., & Ellison, N. (2013). "There's a network out there you might as well tap": Exploring the benefits of and barriers to exchanging informational and support-based resources on facebook. *New Media & Society, 15*, 243–259. http://dx.doi.org/10.1177/1461444812451566.

Walther, J. B. (2011). Introduction to privacy online. In S. Trepte, & L. Reinecke (Eds.), *Privacy online. Perspectives on privacy and self-disclosure in the social web* (pp. 3–8). Berlin u.a: Springer.

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

Xu, H., Rosson, M. B., Gupta, S., & Carroll, J. M. (2012). Measuring mobile users' concerns for information privacy. In *Proceedings of 33rd annual international conference on information systems*. Retrieved from http://faculty.ist.psu.edu/xu/papers/Xu_etal_ICIS_2012a.pdf.