Beyond the Privacy Paradox: Objective versus Relative Risk in Privacy Decision Making

Idris Adjerid*, Eyal Peer**, Alessandro Acquisti***
*University of Notre Dame
**Bar-Ilan University
***Carnegie Mellon University

Abstract:

Privacy decision making has been examined from various perspectives. A dominant "normative" perspective has focused on rational processes by which consumers with stable preferences for privacy weigh the expected benefits of privacy choices against their potential costs. More recently, an alternate "behavioral" perspective has leveraged theories from behavioral decision research to construe privacy decision making as a process in which cognitive heuristics and biases predictably occur. In a series of experiments, we compare the predictive power of these two perspectives by evaluating the impact of changes in *objective* risk of disclosure and the impact of changes in *relative* perceptions of risk of disclosure on both hypothetical and actual consumer privacy choices. We find that both relative and objective risks can, in fact, impact consumer privacy decisions. However, and surprisingly, the impact of objective changes in risk diminishes between hypothetical and actual choice settings. Vice versa, the impact of relative risk is more pronounced going from hypothetical to actual choice settings. Our results suggest a way to integrate diverse streams of IS literature on privacy decision making: consumers may both over-estimate their response to normative factors and under-estimate their response to behavioral factors in hypothetical choice contexts relative to actual choice contexts.

Published Version Can Be Found:
MIS Quarterly
Vol 42 Issue 2, 2018, 465-488
DOI: 10.25300/MISQ/2018/14316

1. Introduction

A significant amount of research across multiple disciplines (such as management and information systems, economics, marketing, psychology, and human computer interaction) has explored consumer privacy decision making. Historically, much of the information systems (IS) research in this area has focused on a "normative" perspective of consumer choice. Normative theories of consumer choice are those consistent with the classical economic view of consumers as deliberative, utility maximizing, rational agents who possess reasonably stable, and therefore predictable, preferences for goods (Simon 1959; Thaler and Mullainathan, 2000). Under this perspective, privacy decisions can be construed as the result of a mental calculus that weighs the expected benefits of privacy allowances against their resulting costs (Klopfer and Rubenstein, 1977; Milne and Gordon, 1993; Dinev and Hart, 2006).

While the importance of privacy risks and benefits in influencing consumer behavior has been proven time and again in the literature (e.g. Marthews and Tucker, 2014), this account of decision making has faced the challenge of explaining surprising, yet robust, empirical occurrences in privacy contexts. This includes the dichotomy between stated privacy attitudes, or stated privacy intentions, and actual behaviors (Spiekermann, Grossklags, and Berendt, 2001 Jensen, Potts, and Jensen, 2005), as well as seemingly contradictory reactions to privacy trade-offs (John, Acquisti, and Loewenstein, 2011; Brandimarte, Acquisti, and Loewenstein, 2013). In the last few decades, a growing body of work in economics and decision research has proposed "behavioral" perspectives on decision making (Thaler and Mullainathan, 2000; Camerer, Loewenstein, and Rabin, 2011). These perspectives are rooted in the notion that systematic, and therefore predictable and replicable, deviations from normative (that is, rational-calculus based) accounts of consumer decision can arise due to limitations in consumers' cognitive ability, or their susceptibility to behavioral heuristics and decision biases. In the privacy context, this perspective suggests that factors independent of both objective trade-offs associated with privacy choices and consumer preferences can still significantly influence consumer behavior. For

example, default options which are trivial to unselect may have a major impact on consumes' privacy choices (Johnson, Bellman, and Lohse, 2002).

Both accounts of privacy decisions stem from legitimate theoretical frameworks and have stimulated considerable bodies of empirical research. However, most of IS privacy research has primarily focused on either the normative *or* behavioral perspectives of privacy decision making. As a result, comparisons between the results produced within the two literatures are *post hoc*, requiring meta-analysis across studies with diverse modeling assumptions and empirical methodologies. Given the significant and growing social and economic implications of consumer privacy decision making, the absence of a bridge between the two streams of work represents a considerable gap in the literature and is thus the focus of this manuscript. We use a series of experiments to investigate normative and behavioral perspectives within the same empirical settings. We evaluate whether these alternative accounts of privacy decision making can both individually account for some of the variation in observed consumer privacy choices. Furthermore, we explore the conditions under which a normative or a behavioral account may differentially explain privacy choices.

We focus on informational privacy, and the impact that different degrees of data protection can have on consumers' willingness to reveal personal information – a construct common in both streams of literature. Across three experiments, we manipulate either normative factors, behavioral factors, or both simultaneously. Many manipulations of either type are available; we lean on the extant privacy and behavioral literatures to identify established manipulations within each perspective to use in our experiments. Specifically, we manipulate a normative factor by varying the objective levels of protection afforded to disclosures of personal information (for instance, whether responses are identified or anonymous). We manipulate a behavioral factor by holding the objective levels of information protection constant, but varying the relative perception of changes in privacy protection afforded to disclosures of personal information, based on seminal research on Prospect Theory and reference dependence

(Kahneman and Tversky, 1979). We capture the impact of these factors on both hypothetical (self-reported) and actual disclosure behavior. This is relevant in light of existing literature suggesting that consumers may both over-estimate their response to normative factors in hypothetical settings due to more favorable beliefs and attitudes about protecting ones' privacy (Ajzen, I., Brown, T. C., and Carvajal, F., 2004) and fail to anticipate the effect of behavioral factors when considering a choice in hypothetical settings (Loewenstein and Adler, 1995; Liberman, Samuels, and Ross, 2004). We explore whether those tendencies result in normative vs. behavioral perspectives having differential effects on hypothetical vs. actual behavior.

Across the experiments, we find evidence that both objective and relative differences in privacy protection impact consumer privacy decisions, lending credence to the notion that both perspectives (normative and behavioral) capture aspects of privacy choice. However, we also find that *objective* privacy protections had a diminished effect on privacy decision making in contexts that involve *actual* privacy choices relative to *hypothetical* privacy choices, whereas *relative* changes in privacy protection had a pronounced effect in *actual* settings relative to *hypothetical* ones. Specifically, we find that in a hypothetical context (Experiment 1), differences in objective privacy protection result in significant differences in participants' reported privacy concerns and their willingness to disclose personal information. In contrast, changes in relative risk result in smaller (although significant) differences in reported privacy concerns, and no differences in hypothetical willingness to disclose personal information. Mirroring what participants were asked to imagine in Experiment 1, in a context with actual disclosures (Experiment 2) we find the opposite effect: differences in objective privacy protection have a small effect on participants' self-disclosure, while relative changes in privacy protections strongly influence participants' propensity for self-disclosure. In a final experiment (Experiment 3), we consider together both normative and behavioral perspectives by manipulating all dimensions simultaneously (objective protection vs. relative protection, and hypothetical vs. actual choice). We find results consistent with the two prior experiments: both objective and relative changes in protection can have an

impact on privacy decision making; however, objective changes have pronounced effects in hypothetical settings, while relative changes have pronounced effects in actual choice settings.

These finding contributes to the IS literature on the drivers and predictors of privacy decision making. While the normative perspective for privacy decision making is now well studied, the behavioral perspective is still developing. While our findings bolster the role of the nascent but growing behavioral perspective, they also provide evidence of the simultaneous (yet uneven) role of both normative and behavioral factors. Such findings have implications beyond the privacy literature. While the study of behavioral factors (such as applications of reference dependence and prospect theory) continues to garner interest from the broader research community across varied contexts,[1] their application to the information systems literature is growing (Herrmann, Kundisch, and Rahman, 2014), but still relatively sparse. This is an area ripe for exploration, considering that many technology choice contexts, related and unrelated to privacy, are highly dynamic, bestowing on prospect theory a potentially important role in understanding consumer decision making in these contexts.

2. Conceptual Background and Theory

A prominent focus of economic research in the last half a century has been understanding the bounds of rational consumer choice and reconciling traditional neoclassical theory with an accumulating body of empirical and theoretical research supporting behavioral accounts of consumer decision making (e.g. Ho, Lim, and Camerer, 2006, Camerer, Lowenstein, and Rabin, 2011). In more recent years, behavioral research has started informing a number of other domains, including information systems. Goes (2013), for instance, highlights the need to incorporate insights from behavioral economics into theoretical and empirical IS research.

The interplay of rational choice and behavioral accounts of decision making is particularly prominent in the context of consumer privacy choice. Extant literature in this area has been

[1] Bartling, Brandes, and Schunk (2015) recently showed that reference dependent decision making seems to hold in the context of coaches and players of professional soccer.

largely predicated around the notion that privacy decision making is largely a rational process driven by what we may refer to as "normative" factors – that is, factors that are normal to consider if an agent is attempting to maximize her utility. Such factors may include the objective benefits and costs of information disclosure, and the agent's stable, coherent preferences (Simon 1959; Thaler and Mullainathan, 2000). For instance, a *privacy calculus* view of consumer decision posits that privacy is subject to interpretation in "economic terms" (Klopfer and Rubenstein, 1977) and that consumer privacy choices are driven by a systematic weighing of the benefits of information disclosures against the perceived privacy risks from such disclosures (Milne and Gordon, 1993; Dinev and Hart, 2006). Along these lines, Westin (2000) posited that most consumers are shrewd privacy balancers who weigh the value to them and society of various business and government programs calling for personal information. Relatedly, a considerable body of work has focused on identifying systematic differences in privacy concerns between consumers (e.g. Smith, Milberg, and Burke, 1996) and has suggested that elevated privacy concerns correspond to privacy seeking behavior, such a diminished willingness to disclose personal information (Malhotra, Kim, and Agarwal, 2004).

A more recent theme in the IS privacy literature has been the focus on factors that ostensibly should have little (or even no) direct impact on objective risk and benefits of disclosure, but which nevertheless considerably impact people's privacy concerns and personal preferences for self-disclosure (e.g., Moon, 2000). For example, people respond more honestly and with higher rates of disclosure to an online version, versus a paper-and-pencil version, of the same questionnaire (Tourangeau, 2004), even though online responses are more likely to be tracked, duplicated, disseminated, shared with or accessed by a larger number of parties than a questionnaire filled out on a single copy of paper. Similar effects emerge when comparing online disclosure to those made during face to face communication (e.g., Harper and Harper, 2006). Also, people seem to rely on contextual cues, such as a survey's look and feel or implicit social norms, when disclosing intimate details about themselves (John, Acquisti, and Loewenstein,

2011). Or, holding objective risk constant, the mere increase in perceived control over who can access and use online personal information can result in an increased likelihood to make sensitive, risky disclosures (Brandimarte, Acquisti, and Lowenstein, 2013). This behavioral perspective suggests that consumer privacy preferences may be malleable rather than stable, and that privacy behavior is not just highly context-dependent (something that may be also predicted by rational calculus-grounded theories of privacy decision making), but can in fact be affected by factors with little relationship to changes in objective trade-offs from disclosure, such as order effects, framing, and other decision heuristics.

Much of the privacy literature has studied consumer privacy decision making by evaluating the impact of varying degrees of privacy protection and assurances on consumers' behavior, often with consumer disclosure or engagement with a commercial entity as outcomes of interest. However, most of privacy IS research has focused on either the normative or behavioral perspectives of privacy decision making. In this manuscript, we study the impact of changes in privacy protection and assurances on consumers' privacy behavior, but consider simultaneously normative and behavioral perspectives. We do so by manipulating either objective changes in privacy protection, or relative changes in perceptions of protection, in two alternative contexts extensively examined in previous research: hypothetical self-disclosure choices (that is, behavioral intentions), and actual disclosure decisions.

2.1. Objective Changes in Privacy Protection

A substantial body of research suggests that changes in expected privacy benefits and risks can affect consumers' observed privacy choices. For example, disclosing personal information can lead to consumer benefits such as an improved experience in retail via customization of products, promotions, and even user interfaces (Ansari and Mela, 2003), enable users to derive personal and economic value from social networks (Ellison, Steinfield, and Lampe, 2007), and underlies business models for online services providing free content and applications (Leontiadis et al., 2012). Similarly, the literature has noted a number of potential risks of loss due to these

information disclosures, which include those stemming from the misuse of disclosed data (Featherman and Pavlou, 2003), sharing of personal information with third parties, or price discrimination as a result of information disclosures (Viswanathan et al., 2007). Prior literature suggests that the relationship between consumers' perceived risk and behavior is critically related to consumer trust, both in terms of its impact on consumers' perception of risk (Kim, Ferrin, and Rao, 2008; Vance, Elie-Dit-Cosaque, and Straub, 2008) and as a mediator explaining why shifts in privacy risk impact behavior. For example, Dinev and Hart (2006) show variation in the perceived risk of a context impacts behavioral intentions both directly and through a strong effect on consumer trust and privacy concern for a particular context.

Within this general paradigm, it follows that privacy protections have the potential to influence consumer privacy decision making via their impact on the perceived risks of misuse of consumers' personal information. For example, Dinev and Hart (2006) suggest that assurances from salespeople can mitigate perceptions of risk – which, in their model, would diminish privacy concerns and increase trust, thus leading to changes in behavior. A number of studies test this conjecture by shifting the objective degree of privacy protection afforded to consumers' personal information and find evidence for various facets of this model of consumer behavior. For instance, Culnan and Armstrong (1999) find that the use of fair information practices by firms can engender trust from consumers, reducing privacy concerns and perceived risks of disclosure. Xu et al. (2009) find that self-regulation and government regulation reduce perceived risk from participating in location-based services and increase consumers' intention to disclose personal information. Miyazaki and Krishnamurthy (2002) find a significant effect of privacy seals on consumer perception of firm privacy practices and their stated willingness to disclose personal information. And Xu et al. (2012) find that industry self-regulation and government regulation reduce consumer privacy concerns.

Using treatments of privacy assurances similar to those employed in this literature, we manipulate the objective degree of protection afforded to consumers' disclosure (e.g. the breadth

of access to personal information and the anonymity of responses) afforded to participants via a "privacy notice" (similar to firm privacy policies). We capture the role of normative factors (objective changes in risks and benefits) on privacy behavior through the following hypothesis:

H1: Changes in objective levels of privacy protection will impact disclosure: lower levels of privacy protection will lead to lower levels of disclosure of personal information.

2.2. Relative Shifts in Privacy Protection

As noted in the Introduction, a growing body of empirical evidence has suggested that behavioral factors with little or no direct impact on objective risk and benefits of disclosure, can in fact considerably impact people's privacy concerns and personal preferences for self-disclosure. Decision biases and heuristics can significantly affect privacy decision making (Acquisti, Brandimarte, and Loewenstein 2015). In addition, scholars have identified significant influences of affect and emotions on consumer privacy judgments (Li, Sarathy, and Zhang, 2008; Li, Sarathy, and Xu, 2011). Within the behaviorally-grounded body of research on privacy, increasing attention has been paid to the fact that privacy judgments can be relative in nature (Acquisti, John, and Loewenstein 2012; Egelman, Felt, and Wagner, 2013): consumers may compare their (current) situation to that of other people, or to their situation in the past, and their decisions may be affected by phenomena such as habituation or coherent arbitrariness. This phenomenon may be particularly salient in privacy contexts where heterogeneity in data practices abound (across firms and over time). For instance, firms that aggregate consumer privacy information often highlight improvements (i.e. relative changes) to consumer privacy over time[2] and sometimes notify consumers of their privacy protections in a manner that highlights the relative privacy gains from their services compared to those of their competitors[3].

[2] Facebook, for example, has been known to advertise updates to privacy policies to highlight gains to consumer privacy: https://www.facebook.com/notes/10150251867797131.

[3] Microsoft's "Scroogled" Ad campaign sought to highlight the privacy protectiveness of their services (e.g. search, email, etc.) relative to those of Google. https://en.wikipedia.org/wiki/Scroogled.

Kahneman and Tversky (1979)'s Prospect Theory (PT) is a useful framework for studying the potentially relative nature of consumer privacy choices. PT posits that consumers evaluate outcomes both with respect to objective levels of consumption and with respect to a reference point, treating outcomes above or below the reference point as gains or losses, respectively. In other words, PT allows for both the impact of objective features of a particular choice context that should influence choice (e.g. price of a product) and the features of a particular context that, according to classic accounts of economically rational decision making (e.g., Von Neumann and Morgenstern, 1944), should not have an impact on behavior. Therefore, PT offers a framework for analyzing and compare the impact of both normative vs. behavioral factors on privacy choice: that is, how objective changes in privacy risk can affect privacy decision making, but also how changes in relative perceptions of privacy risk, in absence of changes in objective risk, can still affect can affect consumer privacy decision making.

Considerable empirical evidence supports the notion of reference dependent decision making, and rules out alternate rational explanations of reference dependence (e.g., lack of information or consumer inexperience with a choice context). For example, Kahneman and Tversky (1979) found that individuals are much more likely to accept a gamble when the choice is framed as avoiding a loss compared to when the objectively equivalent choice is framed as obtaining a gain. Moreover, seminal work on the endowment effect (e.g., Kahneman, Knetsch & Thaler, 1991) highlights significant differences in the amount buyers are willing to pay (WTP) for an item compared to the amount sellers are willing to accept (WTA) for the same item. Such a WTA-WTP gap has been attributed to the difference between buyers' and sellers' reference point: whereas buyers consider the purchase of a new item as a gain, sellers consider it as a loss (e.g., Novemsky & Kahneman, 2005). A similar WTA-WTP gap has also been found to operate in the context of disclosure decisions (Acquisti, John, & Lowenstein, 2013). In fact, recent literature (e.g., Koszegi and Rabin, 2007) has incorporated reference dependence in classical models of consumer utility, allowing for consumer utility to be derived from both objective features of a

choice set and also deviations from a reference point. Simply put, Prospect Theory offers a theoretically and empirically validated framework that offers defensible deviations from normative models of decision making, including those that relate to normative perspectives of privacy decision making.

We use insights from Prospect Theory and the empirical literature on reference dependence to evaluate the impact of relative changes in privacy protection on privacy decision making. Under normative perspectives, identical privacy notices should result, on average, in comparable levels of disclosure irrespective of relative changes in privacy notices. However, under an alternative account of decision making that incorporates reference dependence, consumers would evaluate privacy notices relative to their deviation from a reference point, such as the level of protection they had in the recent past or the one they currently use (i.e., the status quo). We capture the role of behavioral factors (relative changes in risks and benefits) on privacy behavior through the following hypothesis:

H2: Relative perception of the level of privacy protection will influence individual privacy decision making: levels of privacy protection perceived to be higher relative to a reference point will result in higher levels of disclosure of personal information.

2.3. Privacy Behavior in Actual vs. Hypothetical Choice Contexts

Given that compelling accounts and empirical evidence exist for both normative and behavioral perspectives on privacy decision making, it is useful to consider which factors may moderate the effect of objective and relative privacy protection on privacy decision making. One such factor could be whether privacy decision making is being studied in hypothetical settings (and captured in the form of attitudes or behavioral intentions), or in behavioral settings (and captured in the form of actual behaviors and choices). Smith et al. (2011) note that "it is quite common for researchers to measure stated intentions instead of actual behaviors" in the extant literature. On the other hand, the behavioral literature cited previously predominantly uses actual choice as outcomes of interest (see, e.g., John, Acquisti, and Loewenstein, 2011; Acquisti, John, and

Loewenstein 2012; Egelman, Felt, and Wagner, 2013; Brandimarte, Acquisti, and Loewenstein, 2013). Of course, one possibility is that both normative and behavioral factors influence behavior to the same degree in hypothetical and actual choice settings, rendering this empirical distinction between the literatures inconsequential. Alternatively, normative and behavioral factors may play different roles when moving from hypothetical to actual choice settings. This can emerge if consumers either misjudge the impact of normative factors between hypothetical and actual choice settings, if they misjudge the impact of behavioral factors between hypothetical and actual choice settings, or of course both.

We first consider the potential of consumers to misjudge their reaction to normative factors moving from hypothetical to actual choice settings. In the psychology literature, *hypothetical bias* refers to a divergence between behavioral intentions in hypothetical contexts vs. actual behavior in real life settings (LaPiere, 1934; Champ, Bishop, and McCollum, 1996; Murphy, 2005). For instance, Sheeran (2006) finds that individuals overstate their propensity to use condoms, undergo a cancer screening, or exercise in hypothetical relative to the same actual choice settings. FeldmanHall et al. (2012) find that subjects say they will give up more money to spare others from mild electrical shocks than they actually do when the shocks are real. In addition, Ajzen, Brown, and Carvajal (2004) find that individuals significantly overstate their propensity to donate to a scholarship fund in hypothetical vs. actual choice settings. Ajzen, Brown, and Carvajal (2004) explain this intention-behavior by the "activation of more favorable beliefs and attitudes." Specifically, they find that participants in the hypothetical choice setting were significantly more likely to indicate that donating to the fund was a social norm (e.g. more like to indicate that they "should" contribute and that those close to them would do the same). They also found that hypothetical settings elicited more favorable attitude towards donating (e.g. more likely to indicate that the behavior was "good" rather than "bad", "right" rather than "wrong", etc.). If choice contexts that involve protecting ones' privacy carry similar dynamics, then consumers' hypothetical evaluations of high vs. low levels of privacy protection (i.e., our

normative manipulations) may be affected by overly positive attitudes related to protecting one's privacy as well as elevated perceptions of it being a social norm. If these positive attitudes and perceptions of others' behavior do not carry over to actual choice settings (as the literature would suggest), then we may expect consumers to overstate their response to objective changes in privacy protection in hypothetical settings relative to actual ones.

Simultaneously, the impact of behavioral factors may vary when moving from hypothetical to actual behavior. The behavioral economics literature evaluates behavioral factors across hypothetical and actual choice settings and finds that, at a minimum, we can expect behavioral factors to have an impact actual choice settings: Knetsch, Tang, and Thaler (2001) find that the endowment effect is robust to repeat trials in actual choice settings; Lichtenstein and Slovic (1971) show preference reversals consistent with behavioral models of choice using actual behavior; and Pommerehne, Schneider, and Zweifel (1982) conclude that even ''when the subjects are exposed to strong incentives to make motivated, rational decisions, the phenomenon of preference reversal does not vanish."[4] Several works, in fact, have suggested that the impact of behavioral factors may even be pronounced in actual choice settings relative to hypothetical ones. For instance, prior work has documented a hot-cold empathy gap between hypothetical and actual choice settings where consumers are not able to anticipate their future "hot" states in actual choice setting (e.g. the impacts on choosing a health entrée of being hungry) when considering the same choices hypothetically (Loewenstein 2000; Kang and Camerer, 2011). More so, Loewenstein and Adler (1995) find that participants consistently underestimated the impact of being given an item on their subsequent valuation of that item (i.e. the endowment effect); O'Donoghue and Rabin (2000) find that consumers can be naïve in their estimation of their own susceptibility to an immediate gratification bias (i.e. time inconsistent discounting); and Liberman,

[4] Relatedly, the experimental economics literature has questioned the use of hypothetical choice settings, although on different grounds: the absence of real economic tradeoffs in hypothetical settings is seen as likely to produce behavioral intentions that may not match actual behavior because individuals have less to lose (Smith, 1991, Conslik, 1996). This has lead some authors to suggest that non-normative models of behavior may emerge in hypothetical choice settings but may wane in actual choice settings (Plott and Zeiler, 2005). The conclusion has been, however, critiqued and challenged in the literature (Fehr, Hakimov, and Kübler, 2015; Isoni, Loomes, and Sugden, 2011).

Samuels, and Ross (2004) find that participants grossly underestimate subtle framing changes to the labels of choice contexts on their subsequent behavior. Kühberger, Schulte-Mecklenbeck, and Perner (2002) examine differential effects of behavioral factors between hypothetical and actual choice settings using positive vs. negative framing manipulations (manipulations rooted in prospect theory from above) and find an "economic anomaly" in that "real decisions with large amounts do not diminish the framing effect; it may even be stronger than is apparent from hypothetical decisions." Translated to privacy contexts, those findings suggest that consumers may fail to anticipate their "hot" state or susceptibility to behavioral factors (e.g. how privacy choice contexts are framed) when considering hypothetical disclosures relative to actual ones. In sum, this work suggests that behavioral factors may have a pronounced effect on actual relative to hypothetical choice.

Taken together, prior literature suggests a novel account of the influence of normative vs. behavioral factors on consumer privacy decision making. In addition to our formal hypotheses, which test whether both normative and behavioral factors can have an influence on privacy decision making, we explore whether the impact of normative factors (changes in objective protections in our context) may diminish going from hypothetical to actual privacy choices while the impact of behavioral factors (relative changes in protection in our context) may be pronounced going from hypothetical to actual choice contexts.

3. Methods

In three experiments, we evaluate the role of objective changes in privacy protection and of relative judgments of privacy protections on participants' hypothetical and actual privacy-sensitive behaviors (self-disclosures and selections of privacy settings). Experiment 1 is a hypothetical study in which participants are presented with questions of a personal and sensitive nature, and graphical privacy notices are used to manipulate either the objective protection or the *relative* perception of privacy protection afforded to the answers provided by subjects; participants are asked to report both their privacy concerns and their hypothetical disclosure

behavior. Experiment 2 uses a similar context as that of Experiment 1 but captures actual disclosure behavior, and uses textual privacy notices (similar, although simplified, to those used by online services) to manipulate objective and relative changes in privacy protection. Finally, Experiment 3 combines and extends Experiments 1 and 2 by manipulating simultaneously changes in the objective and relative levels of privacy protection, and by capturing both hypothetical and actual behavior.

We measure self-disclosure by capturing participants' answers to questions of personal and sensitive nature. This approach has been used successfully in the past to examine privacy-sensitive behaviors (e.g., Moon, 2001, Acquisti et al., 2012). While the ostensible goal of the studies is to investigate participants' engagements in various behaviors (for instance: "Have you ever looked at pornographic material?"; see examples in Appendix A.2), we are not interested in those behaviors per se, but rather in whether or not participants are willing to disclose information about their engaging in them. As all of our experiments use random assignments to the different conditions, the distribution of participants' actual past engagement in these activities can be assumed to be similar across conditions. Thus, higher or lowers admittance rates across conditions signal an impact of the manipulation on self-disclosure levels.

A strong rationale for this method is its ability to circumvent significant obstacles in obtaining actual self-disclosures from participants. First, it avoids divulging that the goal of the study relates to privacy and self-disclosure, allowing participants to act more naturally without being primed by experimenter demand effects. Second, simply asking participants to disclose sensitive information like SSN or health information may have legal or ethical implications and is difficult to interpret since we cannot ascertain when consumers choose to mask information or disclose it (i.e. we cannot tell the difference between a fake and an actual response if they provide a nine digit number for SSN). Alternatively, it is unlikely that participants with privacy concerns admit to a behavior when they haven't engaged in it (i.e. mask their lack of engagement in a sensitive activity). This leaves admissions in our context as the complement of the sum of (1)

people who did not engage in the behavior (which we assume to be equal across conditions) and (2) those that did not admit to the behavior although they engaged in it. John, Acquisti, and Loewenstein (2011) note that this approach is conservative because the impact of a given experimental manipulation "has to rise above the noise (error variance) produced by differences in true rates of engaging in the behavior across conditions".

Our participants are sampled from two different but complementary online participant pools, allowing us to test the robustness of the findings. We recruited participants for Experiments 1 and 2 from Amazon Mechanical Turk (AMT). Prior research has validated AMT samples as at least as representative as other internet samples, and significantly more representative than student samples (Buhrmester, Kwang, and Gosling, 2011); furthermore, central findings in IS and the decision sciences have been replicated using AMT samples (Goodman, Cryder, and Cheema, 2013; Steelman, Hammer, and Limayem, 2014). Moreover, AMT offers an effective payment and reputation management system that offers researchers the ability to only sample participants of higher quality (Research has shown that targeting these participants ensures high data quality; see Peer, Vosgerau, and Acquisti, 2013). In Experiment 3, we use another crowdsourcing platform called Prolific Academic, which is similar in most respects to AMT, except that participants on that platform only participate in academic research (whereas AMT also offers commercial uses).

3.1. Estimation Approach

Across the three experiments in this manuscript, we evaluate the impact of randomized manipulations on non-repeating dependent variables (e.g. measures of privacy concerns) and repeated measures of information disclosure where a single participant is asked to make a series of hypothetical or actual disclosure decisions. For non-repeated measures, we evaluate the impact of our randomized treatments using the appropriate statistical tests for our variable of interest (e.g. t test, chi-square test, etc.). Our evaluation of participants' disclosure behavior relies on comparably more complex tests. Because participants across all experiments were presented a

series of questions (asking them either to predict their propensity to make, or to actually make, sensitive disclosures), we observe multiple, correlated responses from each single participant. As a result, we use a random effects linear regression model to evaluate differences in average disclosure between conditions.[5] This model accounts for the correlation between responses from a given participant when estimating the variance-covariance matrix of the coefficients, assuming constant correlation ρ between any two answers within a participant (exchangeable correlation structure: Liang and Zeger, 1986). Specifically, we estimate the following general model:

$$Disclosure_{ij} = \beta * Treatment_i + \delta * \boldsymbol{X}_j + \alpha * \boldsymbol{Y}_i + \theta_i + u_{ij}$$

$Disclosure_{ij}$ measures a participant's predicted or actual propensity to disclose sensitive information or admit to sensitive behavior, i = (1,…,N participants), and j = (1,..,k questions). In some specification, we also include $\boldsymbol{X}_j$*:* a vector of controls for different features of the questions asked to participants; for instance, $Intrusive_j$ controls for questions that differ in their intrusiveness. $\boldsymbol{Y}_i$ is a vector with controls for participant specific controls (e.g. age and gender). θ_i is the participant-specific random effect and u_{ij} is the error term. Estimates on randomly assigned treatments ($Treatment_i$) are unbiased as they should be uncorrelated with observed ($\boldsymbol{X}_j$, $\boldsymbol{Y}_i$) and unobserved (θ_i) individual differences and the error term u_{ij}. While our controls are not necessary for the unbiased estimation of the effect of our treatments on disclosure behavior, they are included in some specifications to rule out any breaks in randomization, and account for some of the variation in disclosure behavior between participants.

4. Experiment 1

In Experiment 1, we manipulated, between subjects, either changes in objective levels of privacy protection, or changes in perceived levels of privacy protection (increase or decrease over time)

[5] We use a linear probability model estimation in lieu of a non-linear estimation approach (e.g. logit) for the straightforward interperation of regression coefficients and the flexibility of OLS in analyzing both likert scale dependent variables and binary outcomes. Angrist and Pischke (2008) have shown little qualitative difference between the Logit and linear probability specification.

while actually holding objective privacy levels constant. We used hypothetical willingness to disclose as our key dependent variable.

4.1. Participants

Two hundred and twenty one participants from AMT (M_{female}=37.56%; M_{age} = 29.16, SD_{age} = 9.76) completed the study and were paid $0.30.

4.2. Design and procedure

Participants were asked to provide their personal opinions regarding two surveys that our research group was, ostensibly, planning to conduct. Participants were told that our research group conducts surveys which include sensitive questions on ethical behavior and that the confidentiality protections for these surveys can vary depending on the study. Specifically, participants were asked for their opinions regarding two surveys called Survey A and Survey B. First, participants were given a description of Survey A, including the level of privacy protection of the survey. Protection levels were described using a figure that showed, on five parameters, the degree to which participants' privacy would be protected during the study – for instance, whether certain identifying information would or would not be required (and possibly linked to the answers provided by the participants); or whether the survey offered a particular protection to the answers provided by the subjects. In one condition, the first survey (Survey A) provided a low overall privacy protection level with the "Less Protective" option for four of the five parameters described (see Figure 3a), and in the other condition, the survey provided a high privacy protection level with the "More Protective" option for four of the five parameters described (see Figure 3b). All other details of the survey (length, purpose and payment) were the same in both conditions. Participants were then asked a set of questions that confirmed they had evaluated and understood each dimension of the notice provided (e.g. "Are responses kept after the study ends") They were then asked to report their satisfaction with the protections provided in each survey, their perception of potential harm from disclosure in the study, and their concerns about their privacy (see Appendix A.1). Finally, participants were asked questions gauging their hypothetical

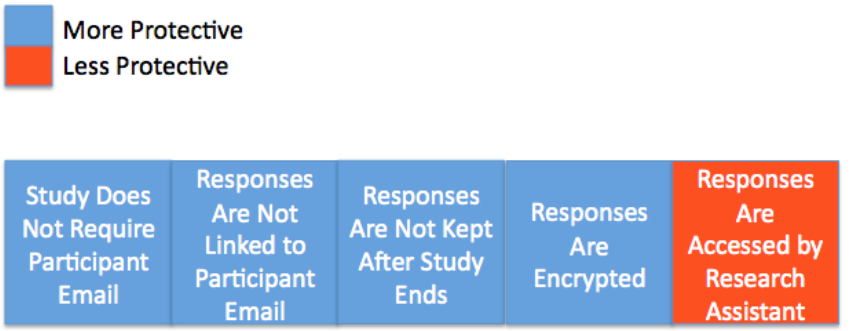
willingness to disclose for descriptive but sensitive information (e.g. address or phone number)[6], and how often had they engaged in a set of potentially sensitive or even unethical behaviors (see Appendix A.2). Similar to the extant literature using hypothetical or intended behavior (e.g. Dinev and Hart, 2006, Xu et al. 2009), we measured their behavioral intention to disclose this information using five point scales ranging from very likely to very unlikely.

Next, all participants proceeded to review a second survey (Survey B) which provided a medium privacy level in both conditions (see Figure 3c). Participants were asked to evaluate Survey B using the same questions as used for Survey A. The level of protections afforded in Survey B was designed so that participants in the first condition would perceive an *increase* in the privacy level from Survey A to Survey B (low to medium), whereas participants in the second condition would perceive a decrease in the privacy level from Survey A to Survey B (from high to medium). We evaluate participants' perception of privacy concern, potential harm to them, and satisfaction with protections in Survey A and B to evaluate whether they indeed perceived a decrease or increase in protections between conditions. Notably, the actual level of privacy for Survey B remained the same for both conditions, although the subjective level of that survey's privacy might have changed.

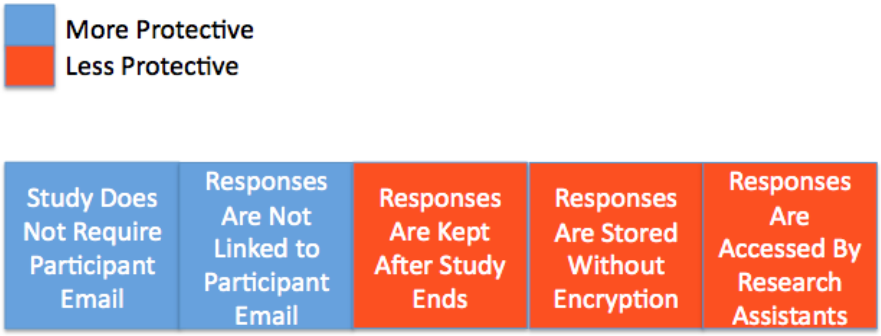
[Figure 1a: Low Protection]

[Figure 1b: High Protection]

[6] These questions were not used in actual disclosure settings since, as we note in our methods section, validation that responses were truthful is not possible.



[Figure 1c: Medium Protection]



4.3. Results

We found that participants, by and large, were able to accurately understand the notices provided in the study. For surveys A and B, 91.85% and 94.57% correctly recalled at least four of the five dimensions. We also found that our manipulation of objective risk using a high and low protection notice (Figure 3a and 3b) was effective at influencing the perception of privacy protection in the first survey (Survey A): Participants provided high protections reported being significantly more satisfied with the protections provided (M_{High}=3.36, M_{Low}=1.56), t (219) = 12.15, $p < .001$, d = 1.64, significantly less concerned about privacy (M_{High}=2.39, M_{Low}=3.87), t (219) = -12.15, $p < .001$, d = 1.64, and significantly less concerned that harm would come them as a result of disclosing personal information (M_{High}=2.86, M_{Low}=4.02), t (219) = -7.46, p <.001, d=1—see Table 1.

We evaluated the impact on participants' predicted disclosure behavior of differences in objective privacy protection using a random effects linear regression estimation approach. Participants reported on a five item scale (1 indicating being "Very Unlikely" to disclose and 5 being "Very Likely" to disclose) their likelihood of disclosure for a given question. We found that

the objective differences in privacy levels in the Survey A had a significant effect on participants' predicted behavior. Participants provided the low privacy level predicted being significantly less likely (β_{Low}= -.67, p=<.001) to disclose personal information (Table 2, Column 1*)*. Moreover, we find consistent results (β_{Low}= -.65, p<.001) when including controls for question type (descriptive vs. ethical) and participants' age and gender (Table 2, Column 2). Broadly, these results provide strong support for the hypothesis that objective risk will impact consumer privacy choice (H1 supported).

[Table 1: Experiment 1 Summary Results]

	Survey A			*Survey B*		
CONDITIONS	High Protection	Low Protection	*p*-value	Increasing	Decreasing	*p*-value
Privacy Concern	2.39	3.87	$p < .001$	2.76	3.29	$p < .01$
Protection Satisfaction	3.36	1.56	$p <.001$	2.86	2.41	$p < .01$
Harm Perception	2.86	4.02	$p <.001$	3.37	3.68	$p = .04$

For the second survey (Survey B), which had an objectively identical medium privacy level (Figure 3c) for both conditions, we found that participants in the increasing protection condition reported being significantly more satisfied with the protections provided (M_{Inc} = 2.86, M_{Dec}= 2.41), t (219) = 2.97, $p < .01$, d = 0.40, less concerned about privacy (M_{Inc} = 2.76, M_{Dec}= 3.29), t (219) = -3.48, $p < .01$, d = 0.47, and less concerned that their responses may be used in way that may harm them (M_{Inc} = 3.37, M_{Dec}= 3.68), t (219) = -2.04, p = .04, d = 0.28. However, the relative change in privacy protection in Survey B did not have a significant effect on participants' predicted disclosure behavior. Specifically, we found that increasing privacy protection did not have a significant effect ($\beta_{Increasing}$= .09, p=.451) on overall predicted disclosure levels (Table 2, Column 3). This result is robust ($\beta_{Increasing}$= .11, p=.363) to including controls for question type and participant age and gender (Table 2, Column 4). In this hypothetical disclosures setting, our results suggest a lack of support for the hypothesis that relative perception of privacy protection will impact behavior (H2 not supported).

[Table 2: Experiment One Regression Results]

VARIABLES	(1) Admit	(2) Admit	(3) Admit	(4) Admit
Low Protection	-0.669**	-0.650**		
	(0.120)	(0.118)		
Increasing			0.0925	0.109
			(0.123)	(0.120)
Descriptive		-0.494**		-0.565**
		(0.0607)		(0.0601)
Age		-0.0132*		-0.0100
		(0.00651)		(0.00680)
Gender		0.130		0.196
		(0.124)		(0.129)
Constant	3.631**	4.173**	3.328**	3.772**
	(0.0701)	(0.229)	(0.0784)	(0.249)
Observations	2,210	2,210	2,210	2,210
Number of id	221	221	221	221

Robust standard errors in parentheses; ** p<0.01, * p<0.05, + p<0.1

4.4. Discussion

The results of Experiment 1 suggest that differences in both objective and relative risk have some effect on participant perceptions of protection in the study, but only objective changes in risk influenced predicted levels of self-disclosure decisions (H1 Supported). In contrast, we don't find differences in predicted levels of self-disclosure after changes in relative risk (H2 Not Supported).

Experiment 1 focused on hypothetical elicitation of privacy choices, which, as discussed previously, may be activate distinct choice processes from actual behavior. While this study only captured hypothetical choice, it provided some initial evidence consistent with our conjecture that the impact of normative factors may be pronounced in hypothetical settings while the impact of behavioral factors may be diminished in hypothetical settings. The evidence provided by Experiment 1 in this regard is of course limited, as we cannot determine whether impacts of objective and relative risk will change or stay constant when shifting to actual self-disclosures. Moreover, Experiment 1 used a graphical representation of privacy protection levels, including a key that alerted participants to riskier uses of their personal information. However, privacy

protections online are often communicated in text based notices, where changes in protection may not be as salient. Finally, the design of Experiment 1 did not allow us to identify the distinct effect of relative increases and decreases in the privacy level. For example, it may be the case that our results were purely driven by decreases in the privacy levels, and that increases in the privacy level did not have an impact. We address these issues in Experiment 2.

5. Experiment 2

Experiment 1 focused on how objective and relative privacy protection impact participants' hypothetical disclosures. In Experiment 2, we examined the role of objective and relative changes in privacy protection on actual disclosures. In addition to evaluating H1 and H2 in actual choice settings, Experiment 2 complements Experiment 1 in other ways. First, we use text based privacy notices. Second, the experimental design allows us to evaluate the unique impact of relative increase and decreases in privacy protection as well as objective changes. Specifically, we asked participants in Experiment 2 to take part in two separate surveys about their personal behaviors. Similarly to Experiment 1, each survey provided different stated levels of privacy protections to participants. Between participants, we kept the objective level of privacy offered by the surveys at the same level (and used as a simple text-based privacy notice), and manipulated whether participants experienced a relative increase or decrease in privacy protection levels. We examined the effects of such changes on actual disclosure behavior. By including accompanying control conditions in which protections did not change, we were able to isolate the specific impact of increases and decreases in privacy levels.[7]

[7] Early analysis of Experiment 2 was included in a short paper focused on the effect of privacy notices, published as part of the ACM proceedings from the 2013 Symposium on Usable Privacy and Security (SOUPS).

5.1. Participants

Four hundred and fifteen participants from Amazon Mechanical Turk (51.61% females, M_{age} = 31.27, SD_{age} = 10.72) completed the study online. The experiment was advertised to participants as two, ostensibly unrelated, surveys on (un)ethical behavior.[8]

5.2. Design and Procedure

Experiment 2 consists of a 2 (high vs. low protection in the first survey) X 2 (high vs. low protection in the second survey) between-subject design. Thus, the study consisted of four groups of participants whose privacy protection either *increased* from the first to the second survey (low protection to high protection: LH), *decreased* (high protection to low protection: HL) or stayed the same (low to low protection: LL or high to high protection: HH).

In the first survey, participants were asked demographic questions, including email address as a mandatory question. Participants were told that we would check the validity of their email addresses prior to approving payment for the study (we did not actually store email addresses). Then, participants were provided with a privacy notice concerning the way their answers to the questionnaire would be stored. To more closely model privacy protections in real world contexts, we presented participants with text notices (as opposed to the graphical notices presented in Experiment 1) focusing on whether their responses would be identified or anonymous (see Appendix A.3 for full text of notices provided). Specifically, participants offered "low" protections were informed that their answers would be linked to their email addresses. Conversely, those offered "high" protection were informed that their answers would not be linked to their email addresses.[9] Participants were then presented with six questions relating to ethically questionable activities (see Appendix A.5 for full set of questions). The questions included a subset of the questions that had been judged in Acquisti et al., (2012) as highly intrusive (e.g. "Have you ever had sexual desires for a minor?").

[8] Participants in Experiment 1 were not able to participate in Experiment 2.
[9] In Experiment 1, participants commented in exist questions that they were most concerned about the propensity of a study to require them to provide email addresses and to link their responses via their email address.

Thereafter, participants were asked to complete an additional survey that followed the same structure as the first survey, but had a different visual design, consistent with the idea that participants were asked to participate in two separate studies (see Appendix A.4). Also, participants were provided two separate confirmation codes to submit in order to receive payment for completing both surveys.[10] In the second survey, participants were again asked for their emails and demographic information. Then, they were given a privacy notice concerning the way their answers to the questions would be stored. As in the first survey, the privacy notice signaled either high protection (not linking responses to emails) or low protection (responses linked to emails). Then, participants were presented with six questions, different from those presented to them in the first survey about other ethically questionable behaviors (see Appendix A.5). Lastly, participants responded to some exit questions that gauged both their perception of whether privacy protections changed in each study (e.g. whether the increased, decreased, or stayed the same, depending on the condition) and their recall of privacy notices in both surveys.

5.3. Results

We found that our manipulations of high and low protection elicited the hypothesized effect, with participants in the high protection conditions reporting significantly higher beliefs that their responses would be linked back to them (M_{High}=.79, M_{Low} =.14), t (411) = 18.81, $p < .001$, d = 1.86), relative to participants in the low protection condition. We first evaluated the disclosure rates of participants in the first survey. We found that participants were statistically more likely to disclose (β_{High} =.05 p = .04) when they were provided with high protection in the first survey (Table 3, Column 1). However, our results were only marginally significant (β_{High} =.04 p = .07) with the inclusion of controls for question intrusiveness, the survey's visual design, and participant demographics (Table 3, Column 2). In the first round, we find initial evidence in support of the hypothesis that objective risk will impact participant behavior.

[10] 99.50% of the participants that completed the exit questions indicated they had participated in more than one study and 96.59% of participants indicated that there were differences between the two studies.

We then evaluated disclosure behavior in the second survey of our experiment, where participants were either presented an increasing, decreasing, or identical protection compared to the first survey. A few participants (11%) were unable to accurately recall the privacy notices (whether protections had increased, decreased, or stayed the same from the first to the second survey) and were excluded from our second survey analysis, leaving 368 usable responses.[11] First, we compared participants that had High Protection in both surveys to participants that had Low Protection in both surveys. For the analysis in the second round, we control for the possible impact of disclosing more in the first survey on second survey disclosures using *Survey1Sharing*, which ranges from a value of zero (for participants that did not admit to any of the behaviors in Survey 1), to a value of six (for participants admitting to all behaviors in Survey 1). In contrast to our results for the first survey, we found no effect of high protection vs. low protection on disclosure (β_{High} = -.003, p = .9) in the second survey (Table 3, Column 3). This result is robust (β_{High} = -.0001, p = .99) to including controls for question intrusiveness, the survey's visual design, and participant demographics (Table 3, Column 4). This suggests that participant sensitivity to different levels of privacy protection diminished over a fairly short period of time (i.e. between the time taken to complete the first and second survey); this results in mixed support for H1.

Second, we evaluated the impact of changing protection on disclosure relative to conditions in which did not perceive an increase or decrease (participants were provided objectively equivalent privacy notices). We found an increase in the propensity to disclose ($\beta_{\text{Increasing}}$ = .06, p =.04) for participants that perceived an increase in protection relative to those whose protections stayed constant. This result is robust to including controls for question intrusiveness, the survey's visual design, and participant demographics (Table 3, Columns 5-6). Conversely, we found a decrease in the overall propensity to disclose ($\beta_{\text{Decreasing}}$ =-.08, p =.006) for participants that perceived a decrease in protection relative to those whose protections stayed constant (Table 3, Column 7). Again, this result was robust to including controls for question

[11] The results remain similar when including these participants.

intrusiveness, the survey's visual design, and participant demographics (Table 3, Column 8). These results suggest that participants' relative perceptions of privacy protection had a consistent impact on disclosure behavior (H2 Supported).

[Table 3: Experiment 2 Regression Results]

VARIABLES	(1) Admit	(2) Admit	(3) Admit	(4) Admit	(5) Admit	(6) Admit	(7) Admit	(8) Admit
High Protection	0.0499*	0.0423+	-0.00336	0.0001				
	(0.0240)	(0.0231)	(0.0278)	(0.0278)				
Increasing					0.0605*	0.0604*		
					(0.0295)	(0.0292)		
Decreasing							-0.075**	-0.071**
							(0.0269)	(0.0271)
Intrusive		0.0758**		-0.111**		-0.113**		-0.086**
		(0.0178)		(0.0271)		(0.0259)		(0.0288)
Age		-0.005**		0.00139		0.00324*		0.000579
		(0.0009)		(0.0016)		(0.0014)		(0.0016)
Male		0.0493*		0.0512+		0.0633*		0.0483
		(0.0232)		(0.0301)		(0.0303)		(0.0307)
Survey Design		0.0379		-0.0120		0.00729		-0.0234
		(0.0231)		(0.0300)		(0.0305)		(0.0276)
Survey 1 Sharing			0.105**	0.105**	0.0950**	0.0973**	0.110**	0.109**
			(0.0093)	(0.0099)	(0.0102)	(0.0105)	(0.0099)	(0.0103)
Constant	0.444**	0.525**	0.0149	0.0206	0.0408	-0.0273	0.000929	0.0265
	(0.0176)	(0.0438)	(0.0273)	(0.0693)	(0.0302)	(0.0654)	(0.0278)	(0.0700)
Observations	2,490	2,454	1,164	1,140	1,158	1,140	1,050	1,032
Number of id	415	409	194	190	193	190	175	172

Robust standard errors in parentheses; ** p<0.01, * p<0.05, + p<0.1

5.4. Discussion

As in Experiment 1, the results of Experiment 2 suggest that both objective and relative changes in privacy protection can impact participants' self-disclosure behavior - even in actual choice settings. However, compared with the results we obtained in Experiment 1 (where we used a hypothetical choice context) we observe in Experiment 2 a reversal in the prominence of effects of relative versus objective changes in protection. Specifically, we found that objective changes in the levels of protection had only a weak initial effect on disclosure (only significant at the 10%

level with controls) and no effect of objective differences in privacy protection on disclosure behavior in second survey (H1 Mixed Support). In contrast, *relative* changes in privacy protection had a significant impact on disclosure behavior (H2 Supported). These findings suggest that participants' propensity to disclose personal information can be influenced by seemingly minor factors such as the relative, instead of the absolute, value of privacy protection; whereas, the impact of objective changes in protection on actual behavior may be more limited. Combining results from Experiment 1 with those from Experiment 2 provides initial evidence that objective and behavioral factors may have differential effects in hypothetical versus actual choice settings. Specifically, the impact of objective changes in protection seem to diminish as we shift to actual choice contexts while the impacts of relative changes in protection seem to become more pronounced as we shift to actual choice settings.

While comparison of effects between Experiment 1 and 2 is an informative data point for the manuscript, the conclusions we can draw from this comparison may be limited. While many variables were kept constant across the two experiments (such as the sampling population, the context of the experiments, and so forth), a number of differences across experiments could limit our ability to make direct comparisons across experiments. For example, the studies used different privacy notices with different types of protection and were conducted at different times. Also, both studies were conducted on Amazon Mechanical Turk, introducing some concern that the effects may only persist with that population. These concerns are addressed in Experiment 3.

6. Experiment 3

The goal of Experiment 3 was to confirm that both behavioral and normative factors can be predictors of privacy decision making, while also more directly comparing their respective impacts across hypothetical and actual choice settings in the same experimental setting. Using the same experimental setting allows us to evaluate the effect of both factors in hypothetical and actual choice contexts while significantly reducing the likelihood of other potential explanations of our effect being due to differences between the two prior experiments. Furthermore, we

recruited a new cohort of participants from a new online recruiting platform (Prolific Academic), to test the robustness of the effects on populations other than AMT.

We recruited participants to take part in what was advertised as two separate studies. The first study served to set the stage in terms of privacy protection, and offered participants either a high or low level of privacy protection (as in Experiment 2), but did not involve any measure of self-disclosure. The second study, as in the previous experiments, offered either high or low levels of privacy protection. The experiment therefore consisted in a four-conditions between-subject design. Along one dimension, we manipulated both actual levels of privacy protections and the relative perceptions of those protections (compared to the level of protection participants received in the previous study). This enabled us to examine how self-disclosure was affected by both actual and relative changes in privacy protections. Along the other dimension, we manipulated whether participants were asked to actually disclose personal information (actual choice setting), or whether they were asked to self-report how likely they would be to answer the self-disclosure questions (hypothetically choice setting). With this design, we can test the robustness of the finding that both objective and behavioral factors influence behavior, and we can directly evaluate the conjecture that objective and relative changes in privacy protection may have differential effects across hypothetical and actual choice settings.

6.1. Participants

We recruited 739 participants (51.7% males, Mage = 29.67, SD = 10.1) from Prolific Academic (www.prolificacademic.ac.uk) who completed the study for 1.5 GBP.

6.2. Design and procedure

Participants were invited to complete two studies (similarly to Experiment 2) which were administered one after the other but had unrelated contexts. In the first study, participants were first given instructions regarding the privacy protections afforded by the study. Participants received information about the settings of the study that signaled either a high or a low protection level for the answers provided in the study, as in Experiment 1 (see Figures 1a and 1b,

respectively). Participants were then asked to rate how high or low they considered the protection offered in the study (on a 5-point Likert scale). In the low protection condition, participants were required to provide their email addresses, to increase the perception that responses may be linked to their identities. All participants then engaged in a filler task that separated the first survey from the second (the filler task consisted in viewing a a 5minute video clip and answering open-ended questions about it).

The second study used a different look and feel (type of font, background color, etc.) than the first study. Participants were first given the information about the level of privacy protections provided in the new study, which was either high or low (see Figures 1a and 1b) and were asked to rate their view of the level of protection from "very low" to "very high." Participants in the low protection condition were again required to provide their email addresses. Next, participants were randomly assigned to either the "actual" or "hypothetical" disclosure conditions. In the actual disclosure conditions, participants were asked to answer five personal and sensitive questions used in Acquisti et al., (2012)—see Appendix A.5. Participants were asked to provide their answers on a 4-point scale that ranged from "never" to "many times", with the fifth option being "I prefer not to say." In the hypothetical disclosure condition, the questions remained the same, but participants were asked to imagine taking part of a study with a certain level of protection afforded to the answers.. Similar to Experiment 1 (and again, in-line with measures used in extant literature), hypothetical behavior participants were told that they would be presented the a set of questions relating to (un)ethical behaviors and asked to indicate their likelihood to admit to such behaviors using a five point scale ranging from "definitely no" to "definitely yes." Finally, participants indicated their age and gender to complete the study.

6.3. Results

In the first study, participants in the high protection condition rated it as offering higher privacy protection (M=3.95 vs. 2.87, SD = 0.93, 1.19, t (737) = 13.75, $p < .001$). Consistent results were found for the ratings of privacy protections in the second study (M=4.00 vs. 2.57, SD = 0.81, 1.28,

t (737) = 18.32, $p < .001$). We thus conclude that our manipulation worked as expected, and turn to examine the effects on actual and hypothetical levels of self-disclosure. We first focus our analysis on those in the hypothetical settings where we considered participants as admitting to the behavior if they responded either with "strongly agree" or "agree" to the question of whether they would admit to a particular behavior. We find statistically significant differences in their hypothetical admission rates between those with objectively different (high vs. low) levels of protection (63% vs. 53%, t(188)=2.01, p=.046). Conversely, we do not find any significant differences in hypothetical admissions when protections are held objectively constant but decrease in relative terms (53% vs. 50%, t(180)=.669, p=.50) or increase in relative terms (63% in both conditions, t(181)=.006, p=.99). These results are robust to alternate measurements for hypothetical admission, including a continuous measure (i.e. 1 to 5 on the Likert scale) and considering those that report being uncertain (neither agree nor disagree) as also admitting to the behavior (see Appendix A6). These results are confirmed in a random effects regression (Table 4). We find that objective difference in protection (High Protection) had a significant effect in the hypothetical context (Column 1) while the relative changes have no effect (Column 2 and 3).

[Table 4: Experiment 3 Hypothetical Choice Results]

	Hypothetical Admissions		
VARIABLES	(1)	(2)	(3)
High Protection	0.0878*		
	(0.0441)		
Decreasing		-0.0305	
		(0.0459)	
Increasing			0.00185
			(0.0433)
Age	-0.00154	-0.000852	-0.000954
	(0.00251)	(0.00231)	(0.00276)
Male	-0.105*	-0.107*	-0.0441
	(0.0453)	(0.0467)	(0.0441)
Constant	0.737**	0.720**	0.718**
	(0.0915)	(0.0910)	(0.0967)
Observations	950	910	915
Number of id	190	182	183

Robust standard errors in parentheses; ** p<0.01, * p<0.05, + p<0.1

Next, we consider participants in the actual disclosure conditions where participants were shown the same exact privacy protections and asked the same questions as their counter-parts in the hypothetical disclosure conditions. For these participants, we considered an admission as any response to our questions that indicated that the participant engaged in a particular behavior at least once (similar affirmative admit rates were used in prior work— John, Acquisti, and Loewenstein, 2011). We find that objective differences (high vs. low) in protection, unlike the hypothetical context, did not have a significant effect on disclosure behavior (65% vs. 59%, t(178) =1.47, p=.15). Conversely, and again in contrast to the hypothetical conditions, we find that those who perceived a relative decrease in protection disclosed significantly less than those that did not perceive a change (49% vs. 59%, t(161)=-2.09, p=.038). Recall that these participants were provided objectively identical protections between these conditions. Finally, similar to the hypothetical context, we identify that the relative increases in protection did not have a significant effect on disclosure (64% vs. 65%, t(201)=-0.35, p=.73), suggesting that the effect increases in privacy protection identified in Experiment 2 may not be robust.

[Table 5: Experiment 3 Actual Choice Results]

	Actual Admissions		
VARIABLES	(1)	(2)	(3)
High Protection	0.0552		
	(0.0410)		
Decreasing		-0.108*	
		(0.0476)	
Increasing			-0.0126
			(0.0354)
Age	0.00143	0.00248	-1.24e-05
	(0.00277)	(0.00232)	(0.00192)
Male	-0.0296	-0.0826+	-0.0321
	(0.0408)	(0.0480)	(0.0366)
Constant	0.594**	0.646**	0.695**
	(0.0959)	(0.0987)	(0.0694)
Observations	895	810	1,010
Number of id	179	162	202

Robust standard errors in parentheses; ** p<0.01, * p<0.05, + p<0.1

These results are confirmed in our random effects regression (Table 5). We find that the objective difference in protection (High Protection) did not have a significant effect in actual behavior (Column 1) while relative changes (specifically, a relative decrease in protection) have a strong observable effect (Column 2).

6.4. Discussion

In Experiment 3, we controlled for a number of factors that varied across Experiment 1 and 2, and continued to find that H1 is supported in hypothetical choice but not supported in actual choice settings while H2 is not supported in hypothetical settings but supported in actual choice settings. Thus, the results bolster the findings from the previous experiments for simultaneous effects of normative (H1) and behavioral (H2) on privacy decision making. They also provide more robust evidence supporting the conjecture of a diminished effect of normative factors in hypothetical relative to actual choice contexts, and a pronounced impact of behavioral factors in hypothetical relative to actual choice contexts. Comparing the Hedge's g (a bias corrected and normalized measure of effect size across experiments—Hedges, 1981) for identical treatments in hypothetical vs. actual choice settings supports the insight: Identical relative decreases in privacy protection in hypothetical choice contexts had a treatment effect of only .09, relative to a .33 treatment effect in analogous actual choice settings. Conversely, identical objective decreases in protection had a treatment effect of .32 in hypothetical choice settings, but a diminished treatment effect of .21 in actual choice settings. Summarizing results across our three experiments highlights our main findings (see Table 6). We consistently find evidence that both normative and behavioral factors can simultaneously influence consumer perceptions of privacy risk and actual privacy choices, but that these effects may emerge differentially across hypothetical vs. actual choice contexts.

[Table 6: Overview of Results]

	Experiment 1	**Experiment 2**	**Experiment 3**	
	Hypothetical Choice	*Actual Choice*	*Hypothetical Choice*	*Actual Choice*

H1: Objective Privacy Protection	Supported	Mixed Support	Supported	Not Supported
H2: Relative Privacy Protection	Not Supported	Supported	Not Supported	Supported

7. Discussion and Conclusions

Our work builds on the IS literature on consumer privacy decision making and the behavioral economics literature on reference dependence and relative judgment.Leaning on proposed models of reference-dependent utility, which account for both the utility from absolute levels of consumption and deviations from a reference point, we present some evidence suggesting that, in the context of privacy decision making, relative changes may have an increasingly important impact on decision making, particularly in actual choice contexts, relative to absolute or objective level of protection provided.

Our results have implications for both theories of consumer privacy behavior and policy efforts. More generally, our results suggest that the behavioral factors we evaluate may be underappreciated by consumers when anticipating their privacy concerns and behavior in hypothetical situations, but may actually be more influential on, and more consistent drivers of behavior in contexts that involve actual privacy behavior. These findings are consistent with the broader psychology and behavioral economics literature (e.g., Lowenstein and Adler, 1995; Gilbert and Ebert, 2002), in that they imply that people may overestimate the impact of normative factors on their hypothetical behavior while underestimating the sometimes powerful impact of decision biases on actual decision making. Our results are consistent with the growing literature on how privacy decision making may be particularly susceptible to deviations from economically rational models of decision making, by not only presenting additional evidence of these deviations but starting to identify the conditions under which these effects are most likely to materialize. Finally, our results start to reconcile some of the dissonance in the privacy literature and help explain early results from the privacy paradox literature (e.g., Spiekermann et al., 2001)

by substantiating a critical link in how limitations in consumer (ir)rationality may be driving the observed dissonance between consumer concerns and hypothetical behavior and actual decision making. We clarify however that pragmatic considerations can lead to the choice of using hypothetical vs. actual choice (e.g. whether it is feasible to observe actual behavior in ones' context of interest) so our focus is not to suggest that one approach is always preferred to the other, but simply to suggest that this distinction could be relevant to the tension between normative and behavioral models of privacy decision making. In fact, our results substantiate that both perspectives are predictive of consumer behavior across both choice settings but that they may simply emerge differentially between them.

Our work has some important limitations however. First, we evaluate specific manipulations of the normative and behavioral perspective, which introduces the question of whether these effects would extend to other manipulations of normative vs. behavioral perspectives. We alleviate some of these concerns by using experimental treatments that vary in how they manipulate these factors (e.g. visual vs. text notice) and focus on manipulations that are well rooted in their respective literatures—Prospect Theory, for example, is a seminal theory in the behavioral economics literature and informs numerous behavioral phenomena. More so, we do not claim that the impact of normative factors are always stronger predictors of behavior in a given contexts. Clearly this claim is problematic since one can arbitrarily alter the strength of any normative or behavioral manipulation such that one dominates in a given setting. Rather, we suggest that the effect of similar or identical manipulation of normative *or* behavioral factors differ as they are assessed in hypothetical vs. actual choice contexts.

Another limitation consists in the experimental nature of the work, with constraints in terms of external validity, due to context and sample selection. In some sense, however, this tension is part of our empirical testing, since we evaluate choice across hypothetical and the more realistic actual choice setting. In any case, we leverage diverse online samples that provide more diverse participant pools to address residual concerns in this regard.

Disentangling these diverging perspectives has implications beyond the academic discourse on consumer privacy behaviors. Hoofnagle and Urban (2014) argue that prominent policy intended to protect consumer privacy are predicated on the notion that consumers are able to consistently and predictably react to changes in normative factors within privacy contexts (e.g. the objective benefits and costs of data allowances and disclosures). Such protections are provided across various contexts and through distinct mechanisms. In some cases, protections are mandated via regulation that covers some subset of personal information such as HIPAA in the U.S. or a more general swatch of consumer personal information such as the EU Data Directive in the European Union. Beyond regulation, protections can be provided to consumer personal information via self-regulatory mechanisms including company privacy notices detailing how use of consumer personal information will be limited and the also choice mechanisms that provide consumers the option to choose their desired degree of privacy protection.

Moreover, the evidence in support of reference-dependent privacy decision making presented in this manuscript has, in itself, considerable implications for firms and policy makers. If consumers' judgments of privacy protections in actual choice contexts are relative rather than absolute, market choices might not necessarily capture or reflect "objective" privacy preferences. For example, if privacy protection is increased from a very low (absolute) level of protection, consumers might consider that as a gain, even though the resulting privacy protection might still be low; and consumers might be more inclined to choose privacy protections that seem more protective (in relative terms) but actually may not be. Conversely, if the level of privacy protection is decreased from a high (absolute) level of protection, consumers might consider that as a loss, and be less willing to use the offered service or disclose personal information, even though the actual level of privacy has remained quite high. These results suggest that policy maker goals of consumer privacy protection through transparency and control mechanisms may not be realized if firms choose to highlight gains and downplay losses to privacy protection over time and among their competitors. However, these results could also present an opportunity for

policy makers to bring attention to high relevance privacy contexts by mandating that firms clearly highlight changes in data practices over time, including decreases in protection. This approach may be particularly effective given that, over time, relative changes in protection in our experiments impacted privacy decision more than the objective risk that participants faced.

The implications for firms seeking value from innovations rooted in the collection of consumer personal information is less clear. Firms that benefit from increased disclosure and allowances by consumers may find some short-term value in presenting notices and choices as relatively "more protective." However, if actual data practices violate consumer expectations for privacy, troublesome and costly privacy incidents may persist, leading to less disclosure and trust by consumers and decreased use in the long term. Moreover, if firms highlight the privacy protective nature of their services relative to their competitors, consumers may have an elevated expectation for privacy which may be inconsistent with actual firm data practices. The increasingly dynamic nature of data practices over time and the heterogeneity of data practices between firms suggests that the relative perception of privacy protection will continue to be an important predictor of consumer privacy decision making, and will thus have significant implications for the effectiveness of tools mandated by policy makers and the mechanisms by which firms solicit privacy-relevant choices.

References

1. Acquisti, A., & Grossklags, J. (2005). Privacy and rationality in individual decision making. IEEE Security & Privacy, 2, 24-30.
2. Acquisti, A., Brandimarte, L., & Loewenstein, G. (2015). Privacy and human behavior in the age of information. Science, 347(6221), 509-514.
3. Acquisti, A., John, L. K., & Loewenstein, G. (2012). The impact of relative standards on the propensity to disclose. Journal of Marketing Research,49(2), 160-174.
4. Ajzen, I., Brown, T. C., & Carvajal, F. (2004). Explaining the discrepancy between intentions and actions: The case of hypothetical bias in contingent valuation. Personality and social psychology bulletin, 30(9), 1108-1121.
5. Ansari, A., & Mela, C. F. (2003). E-customization. Journal of Marketing Research, 40(2), 131-145.
6. Bartling, B., Brandes, L., & Schunk, D. (2015). Expectations as reference points: Field evidence from professional soccer. Management Science.
7. Bélanger, F., & Crossler, R. E. (2011). Privacy in the digital age: a review of information privacy research in information systems. Mis Quarterly, 35(4), 1017-1042.

8. Bhatia, S. (2013). Associations and the accumulation of preference.Psychological review, 120(3), 522.
9. Brandimarte, L., Acquisti, A., & Loewenstein, G. (2013). Misplaced Confidences Privacy and the Control Paradox. Social Psychological and Personality Science, 4(3), 340-347.
10. Buhrmester, M., Kwang, T., & Gosling, S. D. (2011). Amazon's Mechanical Turk a new source of inexpensive, yet high-quality, data?. Perspectives on Psychological Science, 6(1), 3-5.
11. Camerer, C. F., Loewenstein, G., & Rabin, M. (Eds.). (2011). Advances in behavioral economics. Princeton University Press.
12. Camerer, C. F., Loewenstein, G., & Rabin, M.. (2011). Advances in behavioral economics. Princeton University Press.
13. Culnan, M. J., & Armstrong, P. K. (1999). Information privacy concerns, procedural fairness, and impersonal trust: An empirical investigation.Organization Science, 10(1), 104-115.
14. Dinev, T., & Hart, P. (2006). An extended privacy calculus model for e-commerce transactions. Information Systems Research, 17(1), 61-80.
15. Egelman, S., Felt, A. P., & Wagner, D. (2013). Choice architecture and smartphone privacy: There'sa price for that. In The economics of information security and privacy (pp. 211-236). Springer Berlin Heidelberg.
16. Ellison, N. B., Steinfield, C., & Lampe, C. (2007). The benefits of Facebook "friends:" Social capital and college students' use of online social network sites. Journal of Computer-Mediated Communication, 12(4), 1143-1168.
17. Featherman, M. S., & Pavlou, P. A. (2003). Predicting e-services adoption: a perceived risk facets perspective. International journal of human-computer studies, 59(4), 451-474.
18. Fehr, D., Hakimov, R., & Kübler, D. (2015). The willingness to pay–willingness to accept gap: A failed replication of Plott and Zeiler. European Economic Review, 78, 120-128.
19. FeldmanHall, O., Mobbs, D., Evans, D., Hiscox, L., Navrady, L., & Dalgleish, T. (2012). What we say and what we do: the relationship between real and hypothetical moral choices. Cognition, 123(3), 434-441.
20. Gilbert, D. T., & Ebert, J. E. (2002). Decisions and revisions: the affective forecasting of changeable outcomes. Journal of personality and social psychology, 82(4), 503.
21. Goes, P. B. (2013). Editor's comments: information systems research and behavioral economics. MIS quarterly, 37(3), 3-8.
22. Harper, V. B., & Harper, E. J. (2006). Understanding student self-disclosure typology through blogging. The Qualitative Report, 11(2), 251-261.
23. Hedges, L. V. (1981). Distribution theory for Glass's estimator of effect size and related estimators. Journal of Educational and Behavioral Statistics,6(2), 107-128.
24. Herrmann, P. N., Kundisch, D. O., & Rahman, M. S. (2014). Beating Irrationality: Does Delegating to IT Alleviate the Sunk Cost Effect?.Management Science, 61(4), 831-850.
25. Ho, T. H., Lim, N., & Camerer, C. F. (2006). Modeling the psychology of consumer and firm behavior with behavioral economics. Journal of marketing Research, 43(3), 307-331.
26. Hoofnagle, C. J., & Urban, J. M. (2014). Alan Westin's Privacy Homo Economicus. Wake Forest Law Review, 47, 102-316.
27. Hui, K. L., Teo, H. H., & Lee, S. Y. T. (2007). The value of privacy assurance: an exploratory field experiment. Mis Quarterly, 19-33.
28. Isoni, A., Loomes, G., & Sugden, R. (2011). The willingness to pay—willingness to accept gap, the "endowment effect," subject misconceptions, and experimental procedures for eliciting valuations: Comment. The American Economic Review, 101(2), 991-1011.
29. Jensen, C., Potts, C., & Jensen, C. (2005). Privacy practices of Internet users: self-reports versus observed behavior. International Journal of Human-Computer Studies, 63(1), 203-227.
30. John, L., Acquisti, A., & Loewenstein, G. (2011). Strangers on a plane: Context dependent willingness to divulge personal information. Journal of Consumer Research, 37(5), 858-873.

31. Johnson, E. J., Bellman, S., & Lohse, G. L. (2002). Defaults, framing and privacy: Why opting in-opting out1. Marketing Letters, 13(1), 5-15.
32. Kahneman, D., & Tversky, A. (1979). Prospect theory: An analysis of decision under risk. Econometrica, 263-291.
33. Kahneman, D., Knetsch, J. L., & Thaler, R. H. (1991). Anomalies: The endowment effect, loss aversion, and status quo bias. The journal of economic perspectives, 193-206.
34. Kim, D. J., Ferrin, D. L., & Rao, H. R. (2008). A trust-based consumer decision-making model in electronic commerce: The role of trust, perceived risk, and their antecedents. Decision support systems, 44(2), 544-564.
35. Klopfer, P.H. & Rubenstein, D.I. (1977). "The Concept Privacy and its Biological Basis," Journal of Social Issues, 33(3), 52-65.
36. Knetsch, J. L., Tang, F. F., & Thaler, R. H. (2001). The endowment effect and repeated market trials: Is the Vickrey auction demand revealing?. Experimental Economics, 4(3), 257-269.
37. Kőszegi, B., & Rabin, M. (2006). A model of reference-dependent preferences.The Quarterly Journal of Economics, 1133-1165.
38. Leontiadis, I., Efstratiou, C., Picone, M., & Mascolo, C. (2012). Don't kill my ads!: balancing privacy in an ad-supported mobile application market. In Proceedings of the Twelfth Workshop on Mobile Computing Systems & Applications (p. 2). ACM.
39. Liberman, V., Samuels, S. M., & Ross, L. (2004). The name of the game: Predictive power of reputations versus situational labels in determining prisoner's dilemma game moves. Personality and social psychology bulletin,30(9), 1175-1185.
40. Loewenstein, G. (2000). Emotions in economic theory and economic behavior. The American Economic Review, 90(2), 426-432
41. Loewenstein, G., & Adler, D. (1995). A bias in the prediction of tastes. The Economic Journal, 929-937.
42. 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.
43. Marthews, A., & Tucker, C. (2014). Government surveillance and internet search behavior. Available at SSRN 2412564.
44. Milberg, S. J., Burke, S. J., Smith, H. J., & Kallman, E. A. (1995). Values, personal information privacy, and regulatory approaches. Communications of the ACM, 38(12), 65-74.
45. Milne, G. R., & Gordon, M. E. (1993). Direct mail privacy-efficiency trade-offs within an implied social contract framework. Journal of Public Policy & Marketing, 206-215.
46. Miyazaki, A. D., & Krishnamurthy, S. (2002). Internet seals of approval: Effects on online privacy policies and consumer perceptions. Journal of Consumer Affairs, 36(1), 28-49.
47. Moon, Y. (2000). Intimate exchanges: Using computers to elicit self-disclosure from consumers. Journal of consumer research, 26(4), 323-339.
48. Norberg, P. A., Horne, D. R., & Horne, D. A. (2007). The privacy paradox: Personal information disclosure intentions versus behaviors. Journal of Consumer Affairs, 41(1), 100-126.
49. Novemsky, N., & Kahneman, D. (2005). The boundaries of loss aversion.Journal of Marketing Research, 42(2), 119-128.
50. O'Donoghue, T., & Rabin, M. (2000). The economics of immediate gratification.Journal of Behavioral Decision Making, 13(2), 233-250.
51. Smith, H. J., Dinev, T., & Xu, H. (2011). Information privacy research: an interdisciplinary review. MIS quarterly, 35(4), 989-1016.
52. Smith, H. J., Milberg, S. J., & Burke, S. J. (1996). Information Privacy: Measuring Individuals' Concerns About Organizational Practices. MIS quarterly,20(2).

53. Spiekermann, S., Grossklags, J., & Berendt, B. (2001). E-privacy in 2nd generation E-commerce: privacy preferences versus actual behavior. In Proceedings of the 3rd ACM conference on Electronic Commerce (pp. 38-47). ACM.
54. Steelman, Z. R., Hammer, B. I., & Limayem, M. (2014). Data collection in the digital age: innovative alterantives to student samples. Mis Quarterly, 38(2), 355-378.
55. Stutzman, F., Gross, R., & Acquisti, A. (2013). Silent listeners: The evolution of privacy and disclosure on facebook. Journal of Privacy and Confidentiality,4(2), 2.
56. The Federal Trade Commission (FTC). (2012). Protecting consumer privacy in an era of rapid change: recommendations for businesses and policy makers. http://www.ftc.gov/os/2012/03/120326privacyreport.pdf.
57. Tourangeau, R. (2004). Survey research and societal change. Annu. Rev. Psychol., 55, 775-801.
58. 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.
59. Vance, A., Elie-Dit-Cosaque, C., & Straub, D. W. (2008). Examining trust in information technology artifacts: the effects of system quality and culture. Journal of Management Information Systems, 24(4), 73-100.
60. Viswanathan, S., Kuruzovich, J., Gosain, S., & Agarwal, R. (2007). Online infomediaries and price discrimination: Evidence from the automotive retailing sector. Journal of Marketing, 71(3), 89-107.
61. Westin, A. F. (2000). Intrusions: Privacy tradeoffs in a free society. Public Perspective, 11(6), 8-11.
62. Xu, H., Teo, H. H., Tan, B. C., & Agarwal, R. (2009). The role of push-pull technology in privacy calculus: the case of location-based services. Journal of Management Information Systems, 26(3), 135-174.
63. Xu, H., Teo, H. H., Tan, B. C., & Agarwal, R. (2012). Research Note-Effects of Individual Self-Protection, Industry Self-Regulation, and Government Regulation on Privacy Concerns: A Study of Location-Based Services. Information Systems Research, 23(4), 1342-1363.
64. Zeger, S. L., & Liang, K. Y. (1986). Longitudinal data analysis for discrete and continuous outcomes. Biometrics, 121-130.

APPENDICES

A.1 Experiment 1- Summary Questions

Measure	Description
Privacy Concern	I would be concerned about my privacy if I was a participant in this upcoming study.
Protection Satisfaction	I am satisfied with the protections provided in this upcoming study.
Harm Perception	I would be concerned that my responses in this upcoming study could be used to harm me.

A.2 Experiment 1- Disclosure Questions

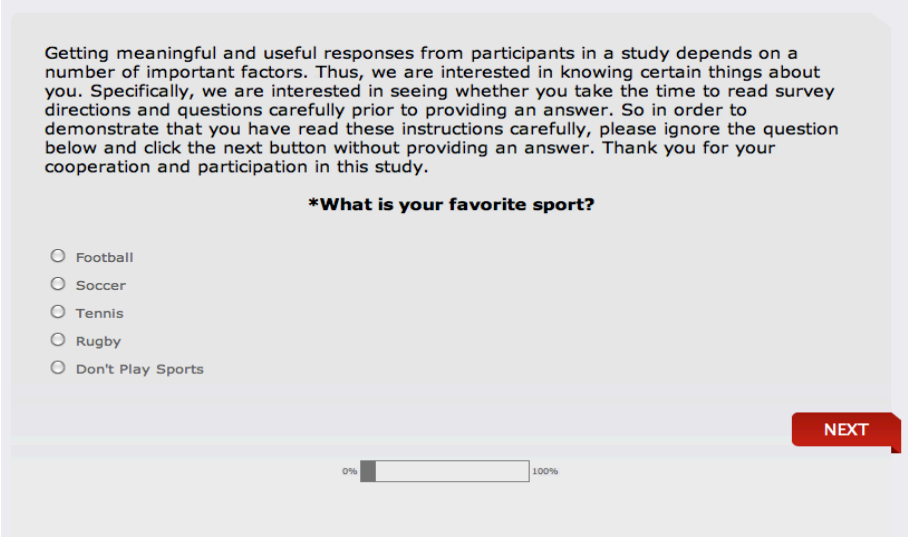
Question	Text	Category
1	What is your annual income?	Descriptive
2	What is your sexual orientation?	Descriptive
3	What is your address?	Descriptive
4	What is your phone number?	Descriptive
5	What is your view on gay rights?	Descriptive
6	Have you every downloaded a pirated song?	Ethical
7	Have you ever flirted with someone other than your partner or spouse?	Ethical
8	Have you ever used drugs of any kind (e.g. weed, heroin, crack)?	Ethical
9	Have you ever looked at pornographic material?	Ethical
10	Have you ever made up a serious excuse, such as a grave illness or death in the family, to get out of doing something?	Ethical

A.3 Experiment 2 Privacy Notice

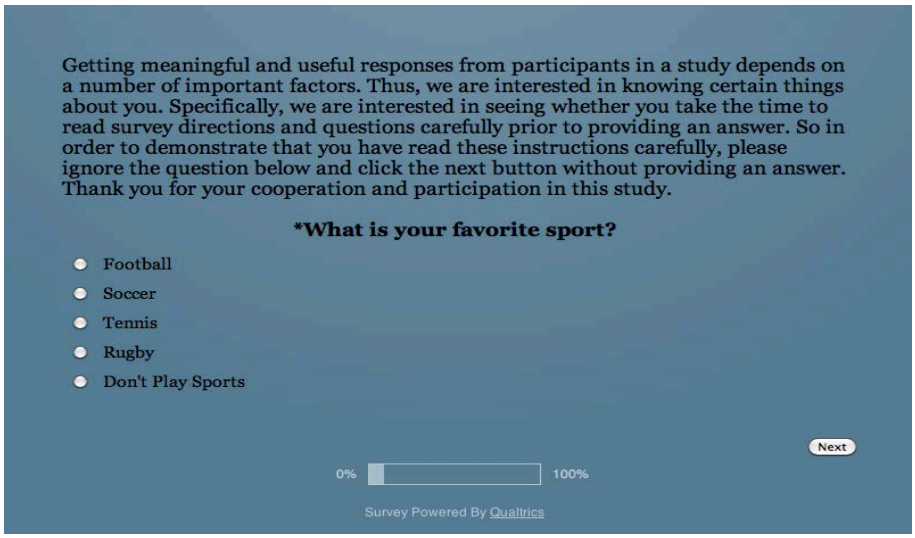
Privacy Notice	Notice Text
High Protection	*The analysis for this study requires that your responses are stored using a randomly assigned ID. All other information that could potentially be used to identify you (email, zip code, etc.) will be stored separately from your responses. As such, your responses to the following set of questions cannot be directly linked back to you.*
Low Protection	*The analysis for this study requires that your responses are stored using your email. As such, your responses to the following set of questions may be directly linked back to you.*

A.4 Attention Check and Study Designs

Design 1 and Attention Check:



Design 2 and Attention Check:



A.5 Experiment Disclosure Questions (Highly Intrusive in Bold)

Question	Text
1*	Have you ever downloaded a pirated song from the internet?
2*	While in a relationship, have you ever flirted with somebody other than your partner?
3	**Have you ever masturbated at work or in a public restroom?**
4	**Have you ever fantasized about having violent nonconsensual sex with someone?**
5	**Have you ever tried to gain access to some else's (e.g. a partner, friend, or colleague's) email account?**
6*	**Have you ever looked at pornographic material?**
7*	**Have you ever used drugs of any kind (e.g. weed, heroin, crack)?**
8	Have you ever let a friend drive after you thought he or she had had too much to drink?
9*	Have you ever made up a serious excuse, such as grave illness or death in the family, to get out of doing something?
10	**Have you ever had sex in a public venue (e.g. restroom of a club, airplane)?**
11	**Have you ever while an adult, had sexual desires for a minor?**
12	**Have you ever had a fantasy of doing something terrible (e.g. torture) to someone?**

*Questions used in Experiment 3

A.6 Analysis using revised measure of Hypothetical Disclosure

Allowing our measure to be both continuous and also include admissions as those indicating they are unsure do not qualitatively change our results: Objective changes have a significant impact on hypothetical behavior while relative changes do not.

	Continuous (Likert)	Revised Binary Measure
Objective Decrease	*3.5 vs. 3.2, $t(188)=-1.9$, $p=.06$	*.6 vs. .69, $t(188)=-2.05$, $p=.04$
Relative Decrease	3.1 vs. 3.2, $t(180)=-.69$, $p=.49$	.56 vs. .6, $t(180)=-.77$, $p=.44$
Relative Increase	3.5 vs. 3.5, $t(181)=-.26$, $p=.79$	.7 vs. .69, $t(181)=-.13$, $p=.91$