Past the Privacy Paradox: The Importance of Privacy Changes as a Function of Control and Complexity

JAMES A. MOUREY AND ARI EZRA WALDMAN

ABSTRACT The privacy paradox is often characterized as a risk-benefit trade-off. Risks like identity theft, invasions of privacy, and online harassment compete with benefits like social need fulfillment, impression management, and self-esteem validation. Individuals' willingness to disclose personal information is thought to vary as a function of this trade-off. Three studies provide initial evidence of an alternative explanation in which one's subjective importance of privacy itself varies as a function of who is in control of managing privacy and the extent to which managing privacy is perceived to be easy or difficult. When privacy is difficult to manage, individuals perceive privacy to be more important when they control privacy management but less important when a social network/company controls privacy management. This changing importance predicts an individual's intentions to disclose private information and moderates established effects that risk-benefit trade-off tolerance and trust in a company's expertise (but not benevolence) have on disclosure.

Although most people say privacy is important, their preferences do not neatly map onto their disclosure behavior: the same people that say they care about their privacy often share a great deal of personal information and put their privacy at risk. This inconsistency is called the "privacy paradox," thought to be the result of a rational risk-benefit trade-off in which individuals ignore their privacy concerns when they feel the benefits of sharing personal information outweigh the risks (Norberg, Horne, and Horne 2007; Li, Sarathy, and Xu 2010). However, research suggests that there are many possible reasons for the privacy paradox. From cognitive scarcity (Veltri and Ivchenko 2017) to cognitive absorption (Alashoor and Baskerville 2015), privacy cynicism (Hoffman, Lutz, and Ranzini 2016) to privacy fatigue (Choi, Park, and Jung 2018), explanations for the privacy paradox extend beyond perceived risks and benefits. We hypothesize that individuals' subjective assessment of the importance of privacy in any given circumstance could change as a function of external factors ignored by the conventional wisdom of the privacy paradox and thereby help predict their likelihood of disclosing personal information.

Our current work offers an alternative explanation for the privacy paradox in which the control over and the complexity of privacy management influences the perceived subjective importance of privacy, in general, and that this shifting importance affects an individual's willingness to disclose private information online. Specifically, when privacy management is perceived to be difficult, the subjective importance of privacy is greater if an individual is in control of privacy management but less important if a technology company is in control of privacy management. The subjective importance of privacy then is likely inversely related to an individual's willingness to disclose private information: when privacy is more important, people disclose less; when privacy is less important, people disclose more.

Across three studies we demonstrate initial support for the proposed shifting importance of privacy explanation and provide evidence of the underlying mechanism via mediation, measured process, and manipulated process. We also then link this subjective importance of privacy hypothesis to established effects in the disclosure literature, like those of the privacy paradox's risk-benefit trade-off tolerance and trust, to show how privacy's shifting importance can moderate these established effects in meaningful ways. The findings have implications for transformative consumer research, particularly with respect to consumer protection: corporate assurances that they will assume more control over privacy management in a world where managing privacy is perceived to be increasingly difficult may ultimately lead to users to share even more private information, thereby putting individuals at greater risk of exploitation.

James A. Mourey (jmourey@depaul.edu) is an assistant professor of marketing at the Driehaus College of Business, DePaul University, 1 East Jackson, Chicago, IL 60604, USA. Ari Ezra Waldman (ari.waldman@nyls.edu) is a professor of law at New York Law School, 185 West Broadway, New York, NY 10013, USA. Authors are listed in alphabetical order, and both authors contributed equally to the project.

JACR, volume 5, number 2. Published online March 13, 2020. https://doi.org/10.1086/708034

THEORETICAL BACKGROUND

Privacy and Control

Privacy is notoriously difficult to define. Privacy scholars have long noted that privacy's complexity and contextuality cannot (and should not) be neatly captured by a single common denominator (Westin 1968; Solove 2008). Privacy includes elements of autonomy, intimacy, dignity, freedom, security, safety, separation, exclusion, limited access, obscurity, and even social values like civility, propriety, and interactional expectations (Fried 1968; Westin 1968; Post 1989; Inness 1992; Nissenbaum 2009; Hartzog and Sellinger 2015; Waldman 2018; Citron 2019). This project does not purport to offer a single definitive conceptualization of privacy, either in all contexts or in the digital world specifically. Nor does it need to. If, as Solove (2008, 40) argues, privacy may be generally understood as a contextual set of expectations and protections against a related cluster of social problems, privacy for the purposes of this study, which focuses on personal disclosure in digital environments, can be defined as the claim of individuals or groups to be free from unwanted access or problems in relation to personal information in online contexts (Hunt 2011).

Effectuating that interest in real life requires active management of privacy-related options and settings. To that end, we define *privacy management* as the sociotechnical process, constrained by design, whereby individuals actively manage settings, options, data storage, and other tactical features in service of privacy maintenance (Hartzog 2018). This includes opting in or opting out of online tracking or targeted advertisement, curating existing data in online contexts, and altering security settings on social media to control who sees what information (Goffman 1959; Fried 1968; Waldman 2018). *Control* over the process of privacy management reflects the extent to which someone is in charge of actively making privacy management choices. In modern online contexts, control over managing privacy can be viewed as belonging more to an individual or to an online company. Along those same lines, *privacy's importance* is defined as the subjective assessment of the value one derives from the perception of being free from unwanted access or problems related to personal information in online contexts. Put another way, privacy is an end, privacy management is one means to that end, control is who actively manages those means, and privacy's importance is how essential that end is in the first place.

In the context of online privacy, individuals have an implicit understanding that platforms will have access to at least some of their information. But the extent to which companies capture user information and the extent of user control over that process is mostly unknown and inscrutable (Pasquale 2015). Recent qualitative research in which 40 undergraduate students from three Midwestern universities were interviewed about their internet and social media behaviors found that young users felt a sense of apathy about their privacy, resigned to the fact that there is not much they could do to protect their privacy even if they wanted to (Hargittai and Marwick 2016). The students spoke of individual control versus a sense of hopelessness when corporations control their information, with some students recognizing that they possessed little-to-no power in comparison to social media and internet companies. Adults experience similar feelings of resignation as well (Turow, Hennessy, and Draper 2015).

Other research exploring privacy online relied on the power-relationship equilibrium (PRE) model to explain the extent to which users were likely to falsify their information, use privacy enhancing technologies, and refuse to purchase or otherwise engage with a website as a function of online privacy concerns (Lwin, Wirtz, and Williams 2007). The PRE model, with roots in sociology and social psychology, suggests that social power and social responsibility are linked such that the more powerful partner in a relationship should bear greater social responsibility to facilitate privacy (Emerson 1962; Murphy et al. 2005). According to this model, individuals may believe that technology companies should bear greater responsibility for protecting privacy insofar as the companies are perceived to have more power.

Of course, the extent to which a social network or company has users' privacy interests at heart is up for debate. On the one hand, prior research incorporating responsibility-alleviation theory—the belief that individuals tend to engage in less risk-taking behavior when they have responsibility over the well-being of others (Charness 2000; Reynolds, Joseph, and Reuben Sherwood 2009)—suggests that individuals might think a technology company will take fewer risks with their personal user information. On the other hand, technology companies depend on steady streams of user data to satisfy an informational capitalist business model based on targeted behavioral advertising, suggesting their interests are at odds with individual interests in privacy (Cohen 2019; Zuboff 2019). Moreover, research exploring the role of locus of control—whether "rewards, reinforcements, or outcomes regarding information . . . are controlled either by one's own actions (internality) or by other forces" (Lo 2010, 3)—suggests that internal control (i.e., personal) would result in lower perceived risk, while external control

(i.e., technology company) would result in higher perceived risk (DuCette and Wolk 1972). Thus, it is not entirely clear how participants perceive privacy risks when they are in control of managing privacy or when technology companies assume privacy management tasks. This perception is complicated by the fact that few people feel they have control over the information collected about them in the first place (Madden and Raine 2015).

The prior research on privacy, in general, and consumer privacy, in particular, highlights the role of control of active privacy management with respect to intentions and behaviors. Whether individuals feel they actively control their privacy management can affect decisions to share information and whether to engage at all. Corporate control over privacy management either increases perceived risk or decreases perceived risk depending on the operating theory. Thus, one purpose of the current work is to explore how control over privacy management affects the perceived importance of privacy in general.

The Privacy Paradox

Prior research exploring information disclosure in online and real-world contexts consistently reveals a discrepancy between individuals' stated preferences and intentions regarding their privacy and their actual behaviors (Barnes 2006; Norberg et al. 2007). In their review, Gerber, Gerber, and Volkamer (2018) found that the theoretical explanation with the strongest empirical evidence was the "privacy calculus" theory, in which individuals engage in a risk-benefit trade-off calculation to determine intentions and ultimate behavior. A different review of more than 32 projects covering 35 competing theories attempting to explain the privacy paradox summarized the phenomenon as being a function of two considerations: (1) a risk-benefit calculation and (2) risk assessment deemed to be none or negligible (Barth and de Jong 2017). Even research-based public policy suggestions bifurcate the privacy paradox into the costs to the consumers and the potential value to the consumers (Caudill and Murphy 2000).

This risk-benefit understanding of the privacy paradox is consistent with prior theorizing, in which the decision to disclose personal information was thought to be the product of a forward-looking, utility-maximizing weighing of pros and cons (Posner 1978a, 1978b; Stigler 1980; Westin 1997; Norberg et al. 2007). However, more recent privacy research suggests that the decision to disclose one's personal information is far less rational and far more nuanced. As Acquisti and Grossklags (2005) argued, rational privacy decision making is hampered by at least three factors: incomplete information, bounded rationality, and systematic psychological deviations from rationality.

Indeed, a growing body of scholarship has shown that an individual's understanding of privacy and her disclosure decisions are influenced by context (Nissenbaum 2004, 2009; Waldman 2018). For example, Acquisti, John, and Loewenstein (2012) found that disclosure behavior is often based on comparative judgments: if individuals perceive that others are willing to disclose, then they too are more likely to disclose. Similarly, John, Acquisti, and Loewenstein (2011) found that individuals are, counterintuitively, more willing to admit to bad behavior on websites that appear unprofessional. These platforms were perceived to be more casual, relaxed, and informal rather than less secure. White (2004) found that individuals' perceptions of their ongoing relationships with consumer organizations and the kind of information companies requested influenced individuals' willingness to disclose. While loyal customers found the exchange of information for commercial benefit generally attractive, they reversed course as soon as companies requested embarrassing data. Other scholars have found that disclosure can also be emotionally manipulated: positive emotional feelings about a website, which were inspired by website design, have been found to correlate with a higher willingness to disclose (Li, Sarathy, and Zhang 2008).

These contextual treatments of the perceived risks and benefits associated with disclosing personal information highlights the importance of thinking about privacy as a situated construct that is dynamic and malleable. Stated differently, rather than thinking of the importance that individuals ascribe to privacy as a fixed, static value, a growing body of research suggests that the subjective importance of privacy can vary over time, across contexts, and as a result of external factors (Nissenbaum 2009). Individuals navigating their privacy are also constrained by the designs of online platforms, which, as science and technology scholars have long noted, constrains the behavior of technology users (Hartzog 2018). Design tricks (so-called dark patterns) limit individuals' ability to translate their privacy preferences into privacy management choices (Mathur et al. 2019). Although, ceteris paribus, the "privacy calculus" of a risk-benefit trade-off may predict an individual's willingness to share in an environment of perfect rationality, other contextual factors, like an individual's subjective perception of privacy's importance in any given moment, may have an impact on her intentions and behaviors. That is, if individuals feel privacy in a particular instance is more important, they would

likely disclose less personal information; but if privacy feels less important at the time, individuals would likely disclose more. The notion that privacy's importance could vary as a function of perceived control over privacy management (e.g., as operationalized by exogenous design facilitators or limitations), and how easy or difficult privacy management is perceived to be is worth exploring. Even holding risks and benefits constant, it may be that an individual's subjective importance of privacy could predict her disclosure intentions and behaviors.

Complexity of Managing Privacy: Feelings as Information

The growth of the surveillance economy has made managing privacy more complex and difficult. Selecting privacy preferences, opting out of behavioral targeting, manifesting consent, and turning off geotracking on the hundreds of websites, apps, and online platforms most people use is burdensome, exhausting, and difficult to manage (Scheibehenne, Greifeneder, and Todd 2010; Hartzog 2018).

It is well established that individuals sometimes rely on their feelings, including feelings of ease or difficulty, when making decisions. The work on metacognitive experience and "feelings-as-information" theory, for example, demonstrates how subjective feelings of ease or difficulty can lead individuals to perceive a stimulus as less risky or riskier, respectively (Song and Schwarz 2009). Similarly, subjective perceptions of importance can vary as a function of the ease or difficulty experienced when engaging in a task (Haddock et al. 1999). Subjective feelings of ease or fluency tend to increase one's tendency to rely on heuristic processing, while subjective experiences of difficulty or disfluency trigger analytical reasoning skills (Alter et al. 2007; Alter and Oppenheimer 2009). This is intuitive—if something feels difficult, it may cue the need to get serious, to engage deeper thought processes, or to give a task or stimulus greater weight—and has been demonstrated in various contexts including education (Diemand-Yauman, Oppenheimer, and Vaughan 2011), culture (Mourey, Lam, and Oyserman 2015), and general decision making (Hernandez and Preston 2013).

The consequences of these effects are not always so straightforward. Consider, for example, how an individual's metacognitive experience of difficulty can both reduce liking for an everyday consumer product by making it seem unfamiliar but enhance liking for a rare product because it seems unique or uncommon (Pocheptsova, Labroo, and Dhar 2010). Similarly, experiences of difficulty have been shown to result in two different interpretations of what that difficulty means: difficulty-as-importance or difficulty-as-impossibility (Oyserman et al. 2018). In their work, Oyserman et al. (2018) showed that students' interpretation of experienced difficulty to mean "important" led to better performance on difficult academic tasks, while the interpretation of experienced difficulty to mean "impossible" led to worse performance on the same difficult task. In the context of the current work, feelings of ease are unlikely to elicit any meaningful differences per the cited processing literature (Alter et al. 2007), but feelings of difficulty should. Even more, when managing privacy is difficult and an individual is in control of managing privacy, this difficulty is likely to be interpreted to mean "important." When managing privacy is difficult but a technology company is in control of managing privacy, this difficulty is likely to be interpreted as "impossible," as the individual has no control over the management of privacy anyway. One goal of the current research is to explore whether the subjective importance of privacy varies as a function of ease/difficulty and who is in control of managing privacy.

Control, Complexity, and the Subjective Importance of Privacy

Given this research context, it is worth studying whether control over, and complexity of, privacy management influence an individual's subjective importance of privacy in a predictable manner (see fig. 1). More specifically, we hypothesize:

> **H1:** The subjective importance of privacy varies as a function of the perceived ease/difficulty of managing privacy and whether oneself or a company is in control of actively managing privacy.

Per the interpretation of difficulty literature (Oyserman et al. 2018) cited above, we further hypothesize:

> **H2:** If managing privacy is perceived to be difficult, then the subjective importance of privacy will be higher (lower) if an individual (online company) is said to be in control of actively managing privacy.

Although prior work has explored the mediating role of trust in a social network (Dwyer, Hiltz, and Passerini 2007), perceived risk (Fogel and Nehmad 2009), and online privacy concern as defined by the apprehension over the use of personal data (Lwin et al. 2007) on site engagement and disclosure, no study has looked at the subjective importance

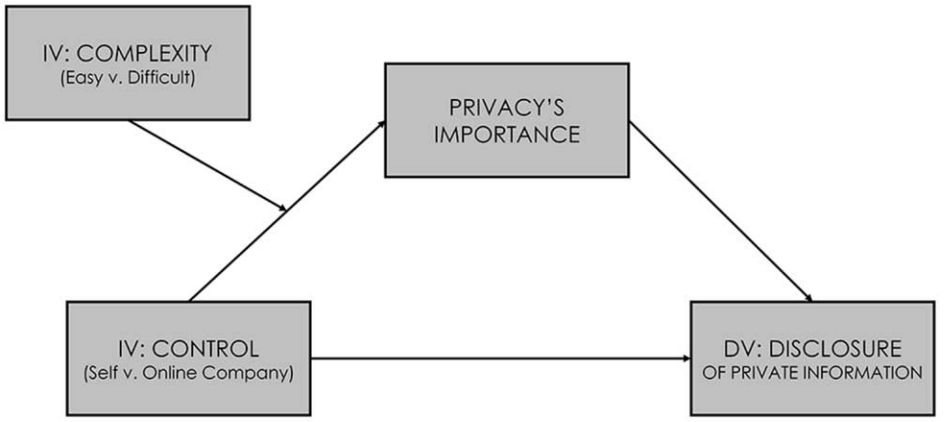

Figure 1. Conceptual model of proposed mediating role of privacy's importance.

of privacy, in general, as a potential mediator between control and complexity and their effect on disclosure. We hypothesize:

H3: Individuals' subjective importance of privacy is inversely related with their intentions to disclose relatively more private, but not more public, personal information: greater (lesser) importance decreases (increases) disclosure of private personal information.

H4: The interaction of control and complexity of managing privacy predicts the subjective importance of privacy, which, in turn, predicts intentions to disclose private information (moderated mediation).

In three studies, we first test the initial hypothesis that control has and the ease/difficulty of managing privacy influence the subjective importance of privacy. We explore this effect using both a news release (experiment 1) and privacy policy (experiment 2) to test the robustness and ecological validity of the effect. In addition, the mediating role of privacy's importance is demonstrated via moderated mediation analysis with effects for willingness to share relatively more private personal information online (experiments 1–2). Next, to provide additional evidence that the subjective importance of privacy is the mechanism underlying the observed effects, the third and final study manipulates privacy's importance directly and, in doing so, both replicates and reverses the findings for intentions to post private personal information. In addition, the final study demonstrates that control and privacy's importance influence people's risk-benefit trade-off tolerance and perceived trust in online companies' expertise, which then affect disclosure intentions. Together, the results provide initial evidence for an alternative explanation for the privacy paradox and, in doing so, motivate future research that can build and expand upon these ideas.

EXPERIMENT 1: NEWS RELEASE

The purpose of the initial experiment was to provide support for the central hypotheses of the current project: first, the subjective importance of privacy varies as a function of who is in control of managing privacy and how easy or difficult privacy is to manage; second, the intention to disclose private information is inversely correlated with this subjective importance of privacy. An additional goal of the first study was to rule out alternative explanations for the hypothesized effect, specifically, differences in benefits from disclosing information, perceived competence, and willingness to engage in risky behavior. To give the current work greater ecological validity, the designs of the stimuli and dependent variables throughout all experiments were inspired by common modern privacy information—press releases, privacy policies, and news stories—and disclosure decisions.

Method

Design and Participants. A total of 211 participants (M_{age} = 36.50, SD_{age} = 11.59; 55% female) recruited from Amazon Mechanical Turk (MTurk) completed the first experiment in exchange for $.25. A sample size target of 200 participants was set in advance. Participants were told they would be completing a survey about social media use and began the survey by selecting which one social media platform they used the most from the following options: Facebook, Instagram, Twitter, Pinterest, LinkedIn, Snapchat,

Tumblr, YouTube, WhatsApp, Other (type name). Their response was piped into the manipulations and dependent measures to make the survey relevant and meaningful, but site selection had no effect on any measure. Participants were then randomly assigned to read one of four news releases that varied on two factors: (1) who was in control of managing privacy (the participant or their selected site) and (2) how easy/difficult managing privacy was to do (see apps. 1, 2; apps. 1–11 are available online). The explicitness of the news releases provided a direct manipulation of the key constructs of control and complexity. For example, in the self/easy condition, participants were apprised of two emerging trends—simpler privacy features and a greater responsibility to manage one's own information—accompanied by short paragraphs detailing these trends. Participants could not advance in the survey until after a 20-second delay to ensure they read the news release.

After reading the news release, all participants proceeded to a new screen that read, "in light of the news release you just read, please review each of the following items and indicate whether or not you would share this information on [selected site]," (9-point scale: −4 = absolutely not, +4 = absolutely yes) followed by a randomized list of 27 items commonly posted to social media (e.g., first and last name, relationship status, views on the news; for the full list see app. 3). Following this, participants were asked, "going forward, do you see yourself using [selected site] less, more, or about the same amount of information on [selected site]?" and "going forward, do you see yourself sharing less, more, or about the same amount of information on [selected site]?" (7-point scales: −3 = much less, +3 = much more). Next, participants indicated the extent to which maintaining privacy and securing their information was important/unimportant (7-point scale: −3 = extremely unimportant, +3 = extremely important), rated the extent to which maintaining privacy was possible/impossible (7-point scale: −3 = completely impossible, +3 = completely possible), and indicated the amount of effort they were willing to put into "maintaining privacy and/or managing their information" (7-point scale: 1 = none, 7 = an extreme amount).

Finally, to rule out possible alternative explanations, five additional measures were included. First, to rule out the possibility that effects were driven by differences in perceived benefits as a function of control and complexity (White 2004), participants were asked, "to the degree that you get something in exchange for sharing your personal information online (e.g., a free email account via Gmail or useful product recommendations on Amazon), how okay are you with sharing personal information if it means getting these benefits?" (5-point scale: 1 = not at all okay, 5 = completely okay). Second, to rule out the possibility that effects were driven by differences in perceived competence between one's self and a company, two questions were added in which participants rated their own competence and their selected social media site's competence with respect to managing privacy (7-point scale: −3 = extremely incompetent, +3 = extremely competent). Finally, to rule out the possibility that effects were due to a difference in willingness to take risks depending on whether oneself or a social media site was in control, two questions were added in which participants rated their willingness to take risks when posting information on social media (7-point scale: −3 = very unwilling, +3 = very willing). Participants completed demographic information and were compensated for completing the survey.

Results and Discussion

Privacy's Importance. Looking first at privacy's importance, the results of a 2 (control: self vs. social network/company) × 2 (complexity: easy vs. difficult) analysis of variance (ANOVA) revealed a significant main effect of complexity ($F(1, 207) = 4.72$, $p < .03$, $\eta^2 = .02$) such that participants felt privacy was more important when told maintaining privacy was easier to do ($M = 2.11$, SD = 1.04) than harder to do ($M = 1.78$, SD = 1.22). Control did not influence importance ($F(1, 207) = .19$, $p = .66$), but a significant interaction of control and complexity emerged ($F(1, 207) = 4.71$, $p < .03$, $\eta^2 = .02$), supporting hypothesis 1 (see fig. 2). Paired contrasts revealed a marginal difference between self and social network/company when privacy management was perceived to be difficult, thereby providing partial support for hypothesis 2 (see table 1). An unpredicted significant contrast emerged for the social network/company as a function of complexity, but no difference emerged between self and social network/company within the easy condition comparisons.

Intentions to Share Content and Use Site. Separate averages for "more public" items ($\alpha = .86$) and "more private" items ($\alpha = .94$) were created per pretest results where participants indicated how public/private each of the 27 shareable items was perceived to be (see apps. 4 and 5). As expected, the intention to share more public items was higher ($M = .77$, SD = 1.72) and the intention to share more private items was lower ($M = -1.18$, SD = 1.82). The intention to share all items fell between the two ($M = -.53$,

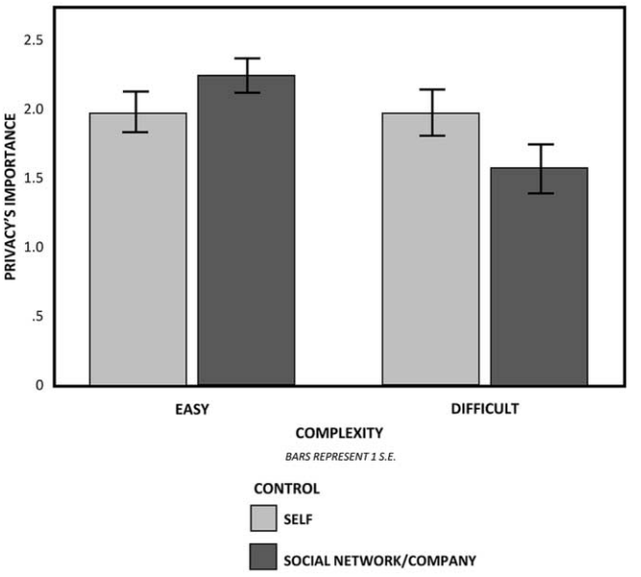

Figure 2. Privacy's importance as a function of control and complexity.

SD = 1.65). No main effects or interaction of control and complexity emerged for the public items, private items, or combination of the two ($F \leq 1.60$, $p \geq .21$). As predicted, privacy's importance was inversely correlated to intention to share private items ($r(211) = -.32, p < .001$) but not public items ($r(211) = .03$, $p = .64$), supporting hypothesis 3.

A test of moderated mediation (model 7 in Hayes 2017) with control and complexity as the predictor variables, privacy's importance as the mediator, and the composite intention to share average for the more private shareable items was marginally significant ($B = .21$; 90% confidence interval [CI]: .01, .43; Savary and Dhar 2014), providing partial support for hypothesis 4, while a follow-up model replacing the dependent variable with the public item composite was not significant (95% CI: −.13, .07). Together, the results suggest that participants who perceived privacy management to be difficult and whom were told they were personally in control of managing privacy rated privacy as being more important and, consequently, had lower intentions to share private information online. Participants who perceived privacy management to be difficult and whom were told their selected social media site was in control of managing privacy rated privacy to be less important, which led to greater intentions to share private personal information online.

Looking next at the single-item measures regarding intentions to use the social media site and to post more or less information going forward, no main effects or interactions of control or complexity were significant for intentions to use the selected social media site or to post more/less information going forward ($F \leq .51$, $p \geq .48$). However, a moderated mediation revealed that privacy's importance marginally mediated the relationship among control, complexity, and intention to share more/less information going forward ($B = .10$; 90% CI: [.01, .22]) following the same pattern as the shared privacy items. Importance did not mediate any effect on intention to use a social media site more/less. Together, results suggest that participants intended to use the site as frequently as one another, but that the amount of information they intended to share varied as a function of control and complexity through the perceived importance of privacy.

Impossibility and Effort. No main effects or interactions were found for the measures of perceived impossibility or effort ($F \leq 2.65$, $p \geq .11$). Neither impossibility nor effort mediated the relationship among control, complexity, and sharing of personal information, whether more public or more private content. However, moderated mediation revealed a marginally significant indirect effect via privacy's importance for effort ($B = -.16$; 90% CI [−.32, −.01]): when managing privacy was perceived to be difficult, participants intended to exert more effort managing privacy if told they were personally in control but less effort if told the social media site was in control. Effort, like private content and

Table 1. Means, Standard Deviations, and Paired Contrasts by Condition for Privacy's Importance

	Complexity		
Control	Easy	Difficult	Paired contrasts (left-to-right)
Self	$M = 1.98$, SD = 1.12	$M = 1.91$, SD = 1.18	$t(207) = .002$, $p = .99$
Social network/company	$M = 2.25$, SD = .93	$M = 1.58$, SD = 1.24	$t(207) = 3.05$, $p < .003$
Paired contrasts (top-down):	$t(207) = -1.23$, $p = .22$	$t(207) = 1.84$, $p = .067$	

intention to share more or less information, varied as function of control and complexity via the perceived importance of privacy. Although prior research (Hargittai and Marwick 2016) suggested a general sense of apathy, the findings for effort here show that users are not universally or consistently apathetic. Instead, efforts to manage privacy vary as a function of control and complexity through privacy's shifting importance: when managing privacy seems difficult, users plan to exert less effort when a company is in control because privacy is perceived to be less important, yet users intend to exert more effort when they are personally in control because privacy is perceived to be more important.

Alternative Explanations. To rule out that the observed effects were due to differences in perceived benefits, perceived competence in managing privacy, or willingness to take risks, five separate ANOVAs were conducted, one for each of the five measures. No main effects or interactions were found for perceived benefits, perceived self-competence, perceived site competence, risk taking if oneself is in control, or risk taking if the social media site is in control ($F \leq 2.13$, $p \geq .15$). Follow-up moderated mediation analyses replacing privacy's importance with each of the alternative explanation metrics also revealed no significant or marginal mediation via the alternative explanation constructs (all confidence intervals included zero at the 95% and 90% significance level). Together, results suggest that differences with respect to intentions to disclose more private personal information, as well the stated intention to share more/less information and to exert effort managing privacy, all vary as a function of privacy's shifting importance and not perceived benefits, competency differences, or risk-taking behavior.

The results of the first experiment provided initial support for the hypotheses that privacy's importance varies as a function of control and complexity of privacy maintenance and that this difference in importance affects an individual's willingness to disclose private but not public information. The results also reveal that effort is not an alternative mechanism but, instead, is also affected by variations in the subjective importance of privacy as a function of control and complexity. Furthermore, control and complexity do not affect individuals' intentions to keep using a social network, in general but do affect how much they intend to share private information going forward. The first experiment also ruled out several alternative explanations—differences in perceived benefits, perceived competence, and willingness to take risks—further supporting the unique role that the subjective importance of privacy plays. Although the first experiment provided preliminary evidence of the hypothesized effect, the experiment relied on an explicit manipulation of control and complexity. A second experiment was designed to explore the robustness of the effect by varying the explicitness of the manipulation, as well as the source.

EXPERIMENT 2: PRIVACY POLICY

The purpose of the second study was to replicate the findings from the first study while also exploring the robustness of the effect by using a different method to manipulate difficulty: the feeling of ease/difficulty stemming from reading a fluent/disfluent privacy policy. That is, instead of explicitly referencing the ease/difficulty of managing privacy as was done in the initial study, the second study explored whether an experience of ease/difficulty with respect to fluency could also produce the effect.

Method

Design and Participants. A total of 200 participants ($M_{age} = 34.51$, $SD_{age} = 10.32$; 58% female) recruited from Amazon MTurk completed the second experiment in exchange for $.25. A sample size target of 200 participants was set in advance. The second experiment was identical to the first experiment with two important exceptions. First, instead of reading news releases that served as explicit condition manipulations, participants were randomly assigned to read one of four privacy policies said to be from their selected site (see app. 6). The policies varied on two factors: (1) who was in control of managing privacy (the participant or their selected site) and (2) how easy/difficult managing privacy felt. Control was manipulated by stating, "On [site selected] you/we are ultimately in charge, where "you" represented the participants and "we" represented the social media company selected. The ease/difficulty factor was manipulated using the complexity of the policy's language (e.g., easy: "from the safety features you select"; difficult: "from your utilization of protectionary attributes") and was supported in a separate pretest (see app. 7). Participants could not advance in the survey until after a 20-second delay to ensure they read the policy. Second, the measures capturing the alternative explanations ruled out in the first experiment were omitted.

After reading the privacy policy, all participants proceeded to a new screen that read, "in light of the privacy policy you just read, please review each of the following items and indicate whether or not you would share this information on [selected site]," followed by the randomized list of 27 items used in the first experiment. Participants also completed the

single-item measures regarding future site use and intention to share more, less, or about the same amount of information on the site, as well as the same importance, impossibility, and effort measures from the first experiment. Finally, participants completed demographic questions and were compensated for participating.

Results and Discussion

Privacy's Importance. Looking first at privacy's importance, the results of a 2 (control: self vs. social network/company) × 2 (complexity: easy vs. difficult) ANOVA revealed a significant main effect of control ($F(1, 196) = 4.24$, $p < .04$, $\eta^2 = .02$) such that participants felt privacy was more important ($M = 2.28$, SD = .85) when told they were in control of establishing and managing their privacy than when told their selected social media site was in control ($M = 1.98$, SD = 1.15). The complexity of the privacy policy did not influence privacy's importance ($F(1, 196) = .001$, $p = .97$). A marginal interaction of control and complexity emerged ($F(1, 196) = 2.67$, $p = .10$) providing partial support for hypothesis 1 (see fig. 3). Paired contrasts revealed this interaction was driven by the predicted difference between self and social network/company control when managing privacy was perceived to be difficult, which provided support for hypothesis 2 (see table 2). The results were consistent with the predicted pattern but suggest the effect may require that individuals perceive actual differences in the difficulty of managing privacy, as shown in the first experiment, instead of more implicit feelings of difficulty elicited via fluency/disfluency.

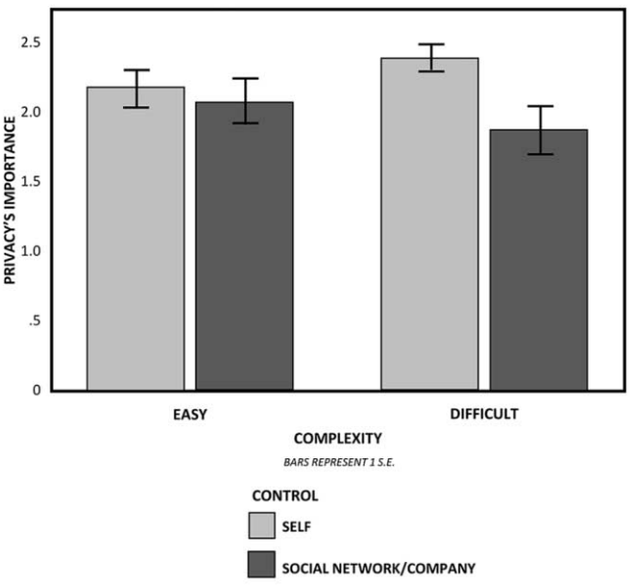

Figure 3. Privacy's importance as a function of control and complexity.

Intentions to Share Content and Use Site. The same composite scores for "more public" items ($\alpha = .90$) and "more private" items ($\alpha = .90$) were created from the intention-to-share ratings as was done in the first experiment, and the same pattern for sharing emerged: the intention to share more public items was higher ($M = .44$, SD = 1.89), private items lower ($M = -1.51$, SD = 1.62), and all items between the two ($M = -.86$, SD = 1.59). Again, no main effects or interaction of control and complexity emerged for the public items, private items, or combination of the two ($F \leq 2.60$, $p \geq .11$). As predicted, privacy's importance was inversely correlated to intention to share private items ($r(200) = -.20$, $p < .004$) but not public items ($r(200) = .05$, $p = .46$), supporting hypothesis 3.

A test of moderated mediation (model 7 in Hayes 2017) with control and complexity as the predictor variables, privacy's importance as the mediator, and the composite intention to share average for the private shareable items as the dependent variable was significant ($B = .16$; 95% CI: .02, 35), providing support for hypothesis 4, while a follow-up model replacing the dependent variable with the public item composite was not significant (95% CI: −.22, . 09). The results replicate those of the first study: when managing privacy is perceived to be difficult, privacy's importance is greater when one is personally in control of managing privacy and lower when a social network/company is in control, and this subjective importance of privacy inversely predicts disclosure of private (but not public) personal information.

Looking next at the single-item measures regarding intentions to use the social media site and to post more/less information going forward, a main effect of control emerged for both site usage ($F(1, 196) = 8.33$, $p < .004$) and intention to post more/less information ($F(1, 196) = 7.61$, $p < .006$): participants who were told they were in control intended to use the site less and post less than participants who were told the social media site was in control. Complexity had no effect on site usage or intention to post more/less information ($F \leq .06$, $p \geq .81$). The interaction of control and complexity on future site use was not significant ($F(1, 196) = 1.33$, $p = .25$) but was significant for intention to post more/less information going forward ($F(1, 196) = 4.07$, $p < .045$). Specifically, participants told they were in control of managing their privacy who perceived privacy management to be difficult intended to post the least ($M = -.90$, SD = 1.53), while participants told the social media site was in control

Table 2. Means, Standard Deviations, and Paired Contrasts by Condition for Privacy's Importance

	Complexity		
Control	Easy	Difficult	Paired contrasts (left-to-right)
Self	$M = 2.16$, SD = 1.01	$M = 2.39$, SD = .67	$t(196) = -1.13$, $p = .26$
Social network/company	$M = 2.10$, SD = 1.07	$M = 1.86$, SD = 1.23	$t(196) = -1.18$, $p = .24$
Paired contrasts (top-down)	$t(196) = .30$, $p = .77$	$t(196) = 2.64$, $p < .009$	

who also saw a difficult privacy policy intended to post the most ($M = .02$, SD = 1.26) with the self/easy ($M = -.49$, SD = 1.31) and site/easy ($M = -.35$, SD = 1.35) between the two. As in the first experiment, a moderated mediation revealed a significant indirect effect via privacy's importance for intention to share more/less information going forward ($B = .16$; 95% CI: .04, 30) following the same pattern as the shared privacy items. Importance did not mediate any effect on intention to use a social media site more/less. Again, although intentions to continue using a social media site did not differ as a function of control and complexity, the intention to share more/less information did differ in the same pattern as before.

Impossibility and Effort. Aside from a marginal main effect of complexity on effort ($M_{\text{difficult}} = 5.46$, SD = 1.17 vs. $M_{\text{easy}} = 5.18$, SD = 1.21; $F(1, 196) = 2.70$, $p = .10$), no main effects or interactions were found for the measures of perceived impossibility or effort ($F \leq 1.00$, $p \geq .32$). Neither impossibility nor effort mediated the relationship among control, complexity, and sharing of personal information, whether more public or more private content. However, moderated mediation through privacy's perceived importance emerged for effort ($B = -.22$; 95% CI: $-.37$, $-.06$): when the privacy policy elicited feelings of difficulty via fluency/disfluency, participants intended to exert more effort on privacy management if told they were in control but less effort if told the social media site was in control, a replication of the initial study's results.

Experiment 2 replicated the findings of experiment 1 using a different, more implicit manipulation of complexity. The marginal control/complexity interaction, while yielding the predicted pattern of results, suggested the effect may be less likely to occur through an experience of ease/difficulty with respect to fluency and may instead require individuals to perceive actual differences in the ease/difficulty of managing the privacy process, as was observed in experiment 1. However, both experiments found that the perceived importance of privacy mediated intentions to disclose more private personal information as predicted. If it is the case that the importance of privacy is the mechanism underlying the observed effects, then directly manipulating privacy's importance should allow for reversal of the effects. For example, the first two studies showed how participants perceived privacy to be less important when managing privacy was said to be difficult and a company was in control, and this lower importance of privacy led to a greater intention to share private personal information. Telling these same participants that privacy is actually very important, then, should reverse the observed effect and decrease these participants' intention to disclose private personal information. A third and final experiment was designed to explore this additional test of the underlying process.

EXPERIMENT 3: MANIPULATING PRIVACY'S IMPORTANCE

The primary purpose of the third and final study was to provide additional support for the subjective importance of privacy as the mechanism underlying the observed relationship among control, complexity, and intention to disclose private personal information. Whereas the first two studies measured the subjective importance of privacy and demonstrated process via mediation, the final study manipulates privacy's importance directly while holding difficulty constant across conditions (as differences are expected when managing privacy is perceived to be difficult, as demonstrated in experiments 1 and 2). Doing so should allow us to replicate and reverse effects observed in the previous studies. A second purpose of the final study was to explore whether privacy's shifting importance could moderate effects of well-known privacy-related constructs, like the privacy paradox's risk-benefit trade-off tolerance and trust, on disclosure intentions. In the case of the privacy paradox, a rational argument would suggest that a higher subjective importance of privacy should lead to lower tolerance for a risk-benefit trade-off (resulting in less disclosure), while a lower subjective importance

of privacy should lead to a greater tolerance for a risk-benefit trade-off (resulting in more disclosure), but is this always true? Thus, a different way to illustrate the unique contribution of privacy's shifting importance to the literature would be to test whether privacy's importance moderates any effects of these existing constructs within the privacy and disclosure literature. Finally, while the first experiment effectively ruled out several alternative explanations, the specific questions were limited in that they were single, standalone measures and, in the case of benefits and risks, were treated separately instead of as the trade-off common to the privacy paradox literature. The final study uses more robust composite measures to rule out alternative explanations including potential differences in self-efficacy.

Method

Design and Participants. A total of 240 participants ($M_{age} = 36.23$, $SD_{age} = 11.23$; 55% female) recruited from Amazon MTurk completed the third experiment in exchange for $.25. A sample size target of 200 participants was set in advance. Participants were randomly assigned to one condition in a 2 (control: self vs. online company) × 2 (privacy's importance: important vs. unimportant) between-subjects design. The results of the first two studies supported the hypothesis that the observed effect should be found when complexity was difficult, so difficulty was held constant across all participants in this final experiment to permit further probing of the effect. Specifically, participants read what was ostensibly an excerpt from a recent newspaper article noting that "actively managing your information, data, and privacy online is difficult," while also varying the extent to which an individual or online companies were in control of actively managing privacy and whether or not privacy was important or unimportant (see app. 8). After reading the news excerpt, participants rated their intention to disclose the 27 shareable items that were used in the first two experiments, as well as their stated intention to share more/less content going forward.

Following these ratings, participants completed additional measures to assess their tolerance for risk-benefit trade-offs, their trust perceptions for themselves and online companies, and their sense of self-efficacy. To measure tolerance for risk-benefit trade-offs, participants rated five related statements including, "I'm willing to share more online if I feel like I'm getting something in return," and "I am okay sharing personal or private information if I get to use email, social media, and other sites for free" (7-point scale: 1 = completely disagree, 7 = completely agree; see app. 9). To measure trust perceptions, participants completed 12 ratings pertaining to the trust components of perceived expertise and benevolence for both themselves (six items) and online companies (six items), which included items like, "how likely are you to say [you/online companies] are knowledgeable about managing data/information and privacy online?"; and "how likely are you to say that [you/online companies] are looking out for your best interests with respect to data/information and privacy online?" (9-point scale: −4 = completely unlikely, +4 = completely likely, see app. 10; White 2005). To measure self-efficacy, participants completed an eight-item self-efficacy inventory (Chen, Gully, and Eden 2001), which included items like, "I believe I can succeed at any endeavor to which I set my mind"; and "when facing difficult tasks, I think I can accomplish them" (5-point scale: 1 = strongly disagree, 5 = strongly agree; see app. 11). Participants completed demographic information and were compensated for completing the survey.

Results and Discussion

Intentions to Share Content. Separate averages for "more public" items ($\alpha = .85$) and "more private" items ($\alpha = .93$) were created. A 2 (control: self vs. online company) × 2 (privacy's importance: important vs. unimportant) ANOVA revealed no significant main effects of control or privacy's importance on intention to share in general, to share public content, or to share private content ($F \leq 1.58, p \geq .21$). Marginal interactions emerged for intention to share private items ($F(1, 236) = 3.63$, $p = .06$, $\eta^2 = .02$) and stated intention to post more/less going forward ($F(1, 236) = 3.56$, $p = .06$, $\eta^2 = .02$). Paired contrasts revealed no significant contrasts for intention to share private items (crossover interaction; see fig. 4, table 3), and one significant contrast for the stated intention to share more/less going forward (see fig. 5, table 4). Replicating the findings of the first two studies, participants intended to disclose more private personal information and to share more, in general, when companies were in control of privacy management and privacy was said to be unimportant. However, when privacy was manipulated to be important, the effects were reversed: participants who thought companies were in control of privacy management intended to disclose less private personal information and to share less information, in general. This finding provides additional support of hypothesis 4, through direct manipulation instead of mediation, by showing how intention to disclose private information is a function of difficulty, control, and privacy's importance. Differences when oneself was in control were less pronounced, but the pattern of means

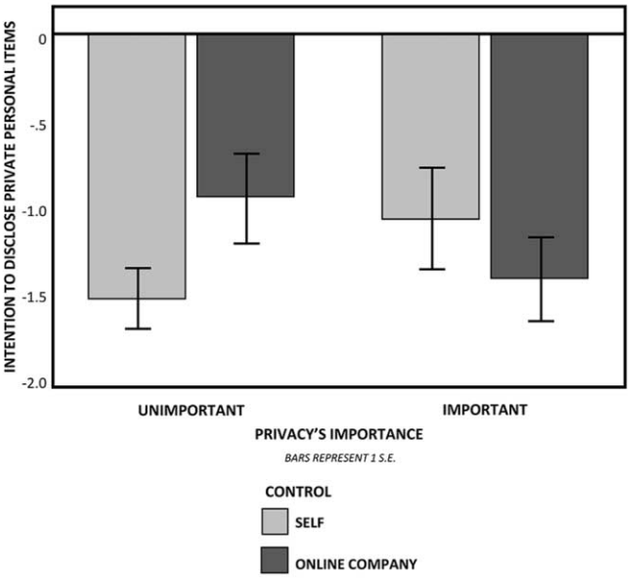

Figure 4. Private item disclosure as a function of control and privacy's importance.

is consistent with the previous experiments' findings: participants share less information and disclose fewer private personal items when privacy is difficult, important, and oneself is in charge compared to participants for whom privacy is difficult, unimportant, and a company is in control.

Risk-Benefit Trade-Off Tolerance. The five privacy paradox risk-benefit trade-off tolerance measures were combined to make a trade-off tolerance composite ($\alpha = .91$). A 2 (control: self vs. online company) $\times$ 2 (privacy's importance: important vs. unimportant) ANOVA revealed no significant main effects of control or privacy's importance on trade-off tolerance ($F \leq .16$, $p \geq .69$). However, a significant interaction emerged ($F(1, 236) = 10.75$, $p < .001$, $\eta^2 = .04$; see fig. 6). Paired contrasts revealed significant contrasts between each paired condition (see table 5). Although a rational approach to a risk-benefit analysis suggests a main effect of privacy's importance on trade-off tolerance (i.e., the more important privacy is, the less tolerant one should be toward trade-offs), none is observed. Instead, the effect of privacy's importance on trade-off tolerance is moderated by who is in control of managing privacy. When privacy is unimportant, people exhibit greater trade-off tolerance when the online company is in control than when they themselves are in control. When privacy is important, people exhibit greater trade-off tolerance when they are in control than when an online company is in control. Thus, it seems one's risk-benefit trade-off tolerance varies as a function of who is control and privacy's varying importance, highlighting the contribution of the latter to the existing work.

A test of moderated mediation (model 7 in Hayes 2017) with control and privacy's importance as the predictor variables, trade-off tolerance as the mediator, and the composite intention to share average for the more private shareable items was also significant (95% CI: $-1.58, -.38$). The results show that when privacy is important, participants intend to disclose fewer private items as a result of having a lower trade-off tolerance when an online company controls privacy management but intend to disclose more private items as a result of having a higher trade-off tolerance when oneself is in control. When privacy is unimportant, participants intend to disclose more private items as a result of having higher trade-off tolerance when an online company controls privacy management but intend to disclose fewer private items as a result of having a lower trade-off tolerance when oneself is control. The pattern of results is consistent with the prior studies' findings for online companies, which makes sense given that one's subjective importance of privacy is lower when a company is in control and privacy management is perceived to be difficult. The results of the current study reflect this for company control, difficulty, and privacy unimportance. The flip for

Table 3. Means, Standard Deviations, and Paired Contrasts for Intention to Share Private Items

	Privacy's importance		
Control	Unimportant	Important	Paired contrasts (left-to-right)
Self	$M = -1.51$, SD = 1.36	$M = -1.05$, SD = 2.22	$t(236) = -1.36$, $p = .18$
Online company	$M = -.94$, SD = 1.89	$M = -1.40$, SD = 1.85	$t(236) = 1.33$, $p = .18$
Paired contrasts (top-down)	$t(236) = -1.67$, $p = .10$	$t(236) = 1.03$, $p = .31$	

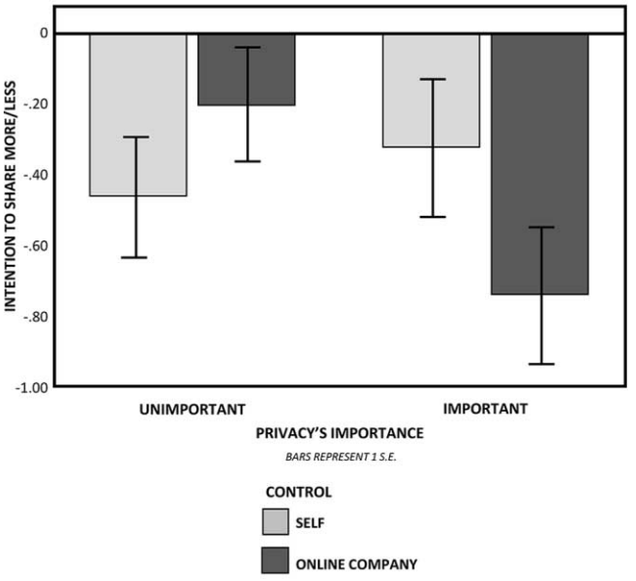

Figure 5. Private item disclosure as a function of control and privacy's importance.

when oneself is in control, although unanticipated, is addressed in the next section.

Trust. The 12 trust measures were combined to make four composite trust scores: Trust_Self_Expertise ($\alpha = .91$). Trust_Self_Benevolence ($\alpha = .83$), Trust_Company_Expertise ($\alpha = .90$), and Trust_Company_Benevolence ($\alpha = .93$). Previous research (White 2005) has shown how participants prefer seeking advice from experts when making less emotionally difficult choices but from more benevolent providers when making more emotionally difficult decisions. Given the technical expertise needed to manage privacy in complicated online contexts, one might expect the opposite to be true here: participants might perceive greater trust in the expertise of an online company when privacy is important and managing privacy is difficult to do. This greater (lower) trust in online companies' expertise is likely to predict intention to disclose more (less) private personal information but only when privacy is important (analogous to the more active, advice-seeking contexts from the motivating literature). A 2 (control: self vs. online company) × 2 (privacy's importance: important vs. unimportant) ANOVA revealed a significant main effect of control on Trust_Company_Expertise ($F(1, 236) = 9.97$, $p < .002$, $\eta^2 = .04$) but no other main effect of control or privacy's importance on any of the other trust scores ($F \leq 2.17$, $p \geq .14$). Participants trusted online companies' expertise more when companies were said to control privacy management ($M = 1.75$, $SD = 1.58$) compared to when oneself was said to control privacy management ($M = .98$, $SD = 2.15$). No interactions between control and privacy's importance emerged across the four dependent trust score measures ($F \leq 2.15$, $p \geq .14$). However, closer inspection of the predicted difference between self and online company control within the important privacy condition revealed a significant planned contrast ($t(236) = -3.29$, $p < .001$; see fig. 7, table 6): when privacy is important, participants exhibited greater trust in the expertise of online companies when these companies were said to be in control of privacy management but less trust in the expertise of online companies when oneself was in control.

A test of moderated mediation (model 7 in Hayes 2017) with control and privacy's importance as the predictor variables, Trust_Company_Expertise as the mediator, and the composite intention to share average for the more private shareable items was significant when privacy was important (95% CI: .06, .40) but not when it was unimportant (95% CI: −.05, .25). Thus, trust in company expertise predicted the relationship between control and intention to disclose private items but only when privacy was important. The pattern of results is consistent with the prior studies' findings for individuals, which makes sense given that one's subjective importance of privacy is higher when oneself is in control and privacy management is perceived to be difficult. The results of the current study reflect this for self-control, difficulty, and privacy importance.

Table 4. Means, Standard Deviations, and Paired Contrasts for Sharing More/Less Going Forward

	Privacy's importance		
Control	Unimportant	Important	Paired contrasts (left-to-right)
Self	$M = -.46$, $SD = 1.34$	$M = -.32$, $SD = 1.50$	$t(236) = -.57$, $p = .57$
Online company	$M = -.20$, $SD = 1.21$	$M = -.74$, $SD = 1.53$	$t(236) = 2.08$, $p < .04$
Paired contrasts (top-down)	$t(236) = -1.02$, $p = .31$	$t(236) = 1.65$, $p = .10$	

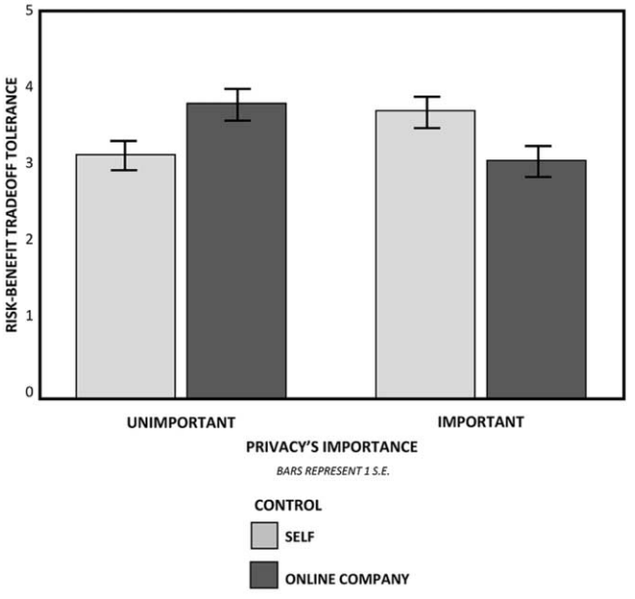

Figure 6. Risk-benefit trade-off tolerance as a function of control and privacy's importance.

Considering the current findings in light of those presented above for trade-off tolerance, it is possible that trade-off tolerance better explains the relationship between privacy's importance and intention to disclose when privacy is less important while trust in an online company's expertise better explains this relationship when privacy is more important. Alternatively, priming consumers to think more about risk-benefit trade-offs or trust in a company's expertise when privacy management is difficult and important could lead them to disclose more or less, respectively. In either case, the findings highlight the importance of better understanding how the subjective importance of privacy plays a role in information disclosure, flipping effects for trade-off tolerance in the former example and moderating effects for trust in company expertise in the current example. These findings highlight the contribution of privacy's shifting importance to the privacy and disclosure literature by showing how the effects of established constructs, like trade-off tolerance and trust (expertise), change as a function of privacy's shifting importance.

Self-Efficacy. The eight self-efficacy measures were combined to make a composite self-efficacy score ($\alpha = .93$). A 2 (control: self vs. online company) $\times$ 2 (privacy's importance: important vs. unimportant) ANOVA revealed no significant main effects ($F \leq .18$, $p \geq .67$). However, a marginally significant interaction emerged ($F(1, 236) = 3.70$, $p = .05$, $\eta^2 = .02$; see fig. 8). Paired contrasts revealed no significant differences (see table 7). A test of moderated mediation (model 7 in Hayes 2017) with control and privacy's importance as the predictor variables, self-efficacy as the mediator, and the composite intention to share average for the more private shareable items was also not significant (95% CI: $-.22$, .07). Self-efficacy, while seemingly affected by control and privacy's importance, does not mediate the relationship between these variables and the intention to disclose private information.

Taken together, the results of the third and final study highlight the importance of understanding the role privacy's importance plays with respect to the disclosure of private personal information. By directly manipulating privacy's importance, results observed in the first two experiments were replicated and reversed as predicted, providing additional support that privacy's importance underlies the observed effects. In addition, linking privacy's importance to the privacy paradox's risk-benefit tolerance trade-off, as well as to a measure of trust (i.e., trust in a company's expertise), shows the nuanced way privacy's changing importance can moderate previously established relationships within the privacy and disclosure literature. With respect to trade-off tolerance, the rational prediction—that a higher (lower) subjective importance of privacy should always lead to lower (higher) tolerance for a risk-benefit trade-off and resulting in less (more) disclosure—is not supported by the results. Instead, trade-off tolerance varies by importance as a function of

Table 5. Means, Standard Deviations, and Paired Contrasts for Risk-Benefit Trade-off Tolerance

	Privacy's importance		
Control	Unimportant	Important	Paired contrasts (left-to-right)
Self	$M = 3.14$, SD = 1.48	$M = 3.72$, SD = 1.55	$t(236) = -2.06$, $p < .04$
Online company	$M = 3.81$, SD = 1.58	$M = 3.08$, SD = 1.61	$t(236) = 2.57$, $p < .01$
Paired contrasts (top-down)	$t(236) = -2.35$, $p < .02$	$t(236) = 2.28$, $p < .02$	

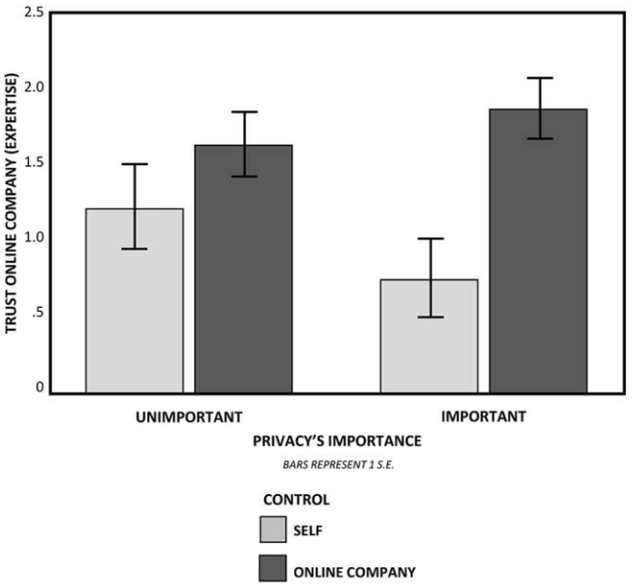

Figure 7. Trust online company (expertise) as a function of control and privacy's importance.

who is in control of managing privacy. The malleability of privacy's importance, as demonstrated by the interaction of control and complexity of privacy management in the first two studies, suggests that a better understanding of the relationships among these important influencers of disclosure is possible and worthy of future exploration.

GENERAL DISCUSSION

Much of modern life is intermediated by online platforms that collect our data. From social media to free email accounts, online shopping to social browsing, individuals are constantly confronted with data collection and privacy management moments. Legislative attempts to protect privacy—which include proposals to give individuals more "control" over their privacy, impose affirmative obligations on technology companies, and everything in between—are often rejected or ignored by the discourse of the "privacy paradox": people don't care about their privacy, the argument goes, because they freely disclose significant amounts of information online. As public policy shifts expectations for who controls (or actively manages) privacy, and technology either makes controlling privacy feel more easy or difficult to do, better understanding individuals' subjective importance of privacy has never been more important.

Three experiments provide initial support for the proposed subjective importance of privacy hypothesis that suggests control and complexity of managing privacy shifts individuals' subjective perception of the importance of privacy, which then influences their willingness to disclose private personal information. The process underlying the effect—differences in the subjective importance of privacy—is demonstrated via statistical mediation and by direct manipulation of privacy's importance. The direct manipulation of privacy's importance allows for both replication and reversal of observed effects, providing additional evidence that privacy's importance underlies the effects observed throughout. Although effects replicate across studies and the patterns of means emerge as predicted, some limitations exist with respect to robustness: relatively more implicit manipulations of difficulty, such as the ease/difficulty elicited from fluency/disfluency, appear to attenuate results. Thus, while the current studies present initial support for the current work's novel conceptual framework, future research can build on the findings herein to better understand the influence of privacy's shifting importance with respect to privacy and disclosure.

When considering the subjective importance of privacy hypothesis in light of the established work on the privacy paradox, seemingly irrational outcomes emerge. First, the finding that explicit ease/difficulty and implicit feelings of ease/difficulty elicit comparable effects that vary in strength (experiments 1 and 2) is useful. Second, although a rational argument would predict a lower (greater) risk-benefit trade-off tolerance when privacy is said to be important (unimportant), the current work finds that this, too, is more nuanced:

Table 6. Means, Standard Deviations, and Paired Contrasts for Trust Online Company (Expertise)

	Privacy's importance		
Control	Unimportant	Important	Paired contrasts (left-to-right)
Self	$M = 3.14$, SD = 1.48	$M = 3.72$, SD = 1.55	$t(236) = 1.37$, $p = .17$
Online company	$M = 3.81$, SD = 1.58	$M = 3.08$, SD = 1.61	$t(236) = -.71$, $p = .48$
Paired contrasts (top-down)	$t(236) = -1.19$, $p = .23$	$t(236) = -3.29$, $p < .001$	

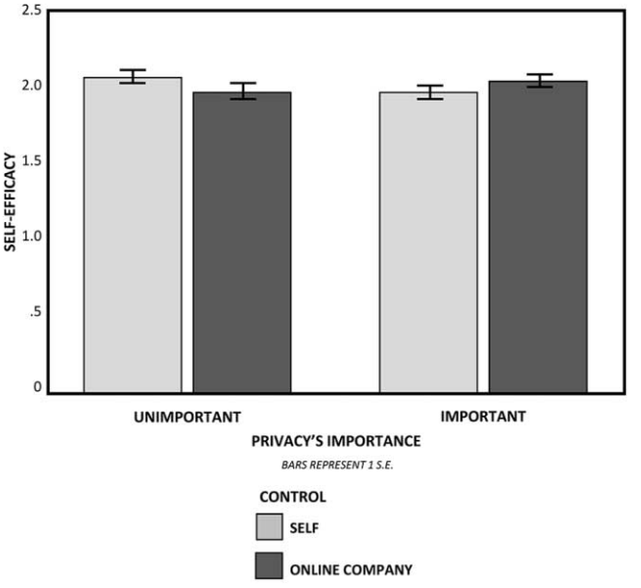

Figure 8. Self-efficacy as a function of control and privacy's importance.

people's trade-off tolerance varies as a function of who controls privacy management and whether privacy perceived to be more or less important (experiment 3). Even effects of trust in a company's expertise are moderated by privacy's shifting importance (experiment 3).

In other words, whereas the conventional wisdom around the "privacy paradox" suggests that individuals make rational disclosure choices, the current work adds to the research offering alternative explanations for the paradox by suggesting that privacy's importance varies among different contexts and predicts disclosure intentions beyond the traditional risk-benefit calculation. More specifically, an important contribution of the current work with respect to the existing literature is that privacy's importance is not a fixed construct but, instead, varies and shifts based on situational factors like who is in control of managing privacy and the ease/difficulty of managing privacy in particular contexts. This finding is particularly striking: corporate pronouncements about their privacy responsibilities together with inscrutably designed privacy management tools may have the effect of actually increasing user tendency to disclose relatively more private personal information.

Theoretical and Practical Contributions

The current work complements and builds on the privacy decision making and disclosure literature. The "privacy paradox" and its correlative assumptions of rational, risk-benefit decision making have long held sway in the literature on privacy and disclosure. In fact, privacy policies are rooted in this "notice and consent" approach, in which companies provide notice of the risks and benefits associated with using their site or services and users consent accordingly. However, this approach has not only been proven inadequate to protect privacy (Reidenberg et al. 2014), but it also reflects outdated assumptions about user behavior. The current research, like that of White (2004), Acquisti and Grossklags (2005), John et al. (2011), and others suggests that disclosure behavior is contextual rather than static, influenced by irrationality rather than pure rationality. Unlike the previous literature, however, we offer another explanation suggesting that perceptions of control and privacy's importance can affect individuals' propensity to disclose private information.

This research also contributes to the literature on the impact and effect of endogenous versus exogenous control with respect to privacy. The literature on the connection between control and risk is split between theories based on responsibility for others and locus of control. Under the former approach, exogenous control over privacy should, theoretically, cause users to perceive lower disclosure risk because those responsible for others tend to take less risks (Charness 2000; Reynolds et al. 2009). Under the latter approach, endogenous control by users themselves should create feelings of empowerment, leading to more confidence in their

Table 7. Means, Standard Deviations, and Paired Contrasts for Self-Efficacy

	Privacy's importance		
Control	Unimportant	Important	Paired contrasts (left-to-right)
Self	$M = 4.12$, SD = .62	$M = 3.91$, SD = .71	$t(236) = 1.68$, $p = .09$
Online company	$M = 3.93$, SD = .76	$M = 4.05$, SD = .66	$t(236) = -1.05$, $p = .30$
Paired contrasts (top-down)	$t(236) = -1.56$, $p = .12$	$t(236) = -1.16$, $p = .25$	

disclosure risks (Lo 2010). The current work suggests that when privacy management is perceived to be difficult, endogenous or personal control increases the perceived subjective importance of privacy and, therefore, decreases disclosure of private personal information. When privacy management is perceived to be difficult, exogeneous control decreases the perceived importance of privacy and increases disclosure of private personal information. The current research provides an explanation for how control can either increase or decrease privacy's importance as a function of the difficulty of privacy management.

That the effects herein manifest when privacy management feels difficult is in line with previous literature on metacognitive experience and cultural fluency (Schwarz 2011; Mourey et al. 2015), which have associated difficulty with greater mental effort and ease or fluency with lower expenditure of effort. Easy experiences do not command the same attention as difficult ones. Similarly, experiences of difficulty can be interpreted to mean a task at hand is important or unimportant, even impossible (Oyserman et al. 2018). In the current context, privacy management is difficult. Effectively navigating the site-by-site and app-by-app privacy permissions can prove exhausting, if not wholly self-defeating (Hartzog 2018). And understanding the data collection effects of particular privacy management choices is difficult even for experts (Reidenberg et al. 2015). Therefore, in a context where perceptions of difficulty are likely to be high, the current work highlights the importance of control, perceptions of difficulty, and privacy's shifting importance in many privacy and disclosure situations.

Our work also has implications for transformative consumer research. Transformative consumer research is work that seeks to benefit consumer welfare and the quality of life for all beings affected by consumption. By showing the impact of control and privacy management complexity on disclosure behavior, the current work can support regulatory efforts to protect consumers and hold technology companies accountable for data misuse. This research suggests technology companies can effectively induce disclosure by design, or, in other words, use code, language, and aesthetics (Hartzog 2018) to make privacy management feel difficult and wrest control away from users. Even a well-intentioned company seeking to reassure users that their data is being properly managed by the company may inadvertently be encouraging users to disclose more information, particularly more private information. In light of these findings, regulators at the Federal Trade Commission (Solove and Hartzog 2014) or in state attorneys-general offices (Citron 2017) should consider and interrogate this possibility of this influence.

Limitations and Future Research

The current work provides initial evidence for the proposition that the control over and perceived difficulty of privacy management have significant effects on perceptions of privacy's importance, which, in turn, influences disclosure behavior. One limitation of this research is that privacy's importance can be influenced by any number of contextual factors not incorporated into the current studies. From relative expertise to perceived confidence, misattributed physiological arousal to emotional state, any number of situational factors could also affect the perceived importance of privacy. We observe this in the final experiment in which both trade-off tolerance and trust in a company's expertise mediated the relationship among control, privacy's importance, and intention to disclose private personal information. Future studies can build on the current work by exploring these relationships to understand when, or why, one process is more likely to elicit an effect than others.

In addition, although the current studies managed to produce the predicted effects using different stimuli, the results were notably weaker when ease/difficulty was manipulated more implicitly via the fluency/disfluency of a privacy policy. This suggests that the proposed effects may require that individuals perceive actual differences in the ease/difficulty of privacy management as opposed to general "feelings of ease/difficulty" elicited by the fluency/disfluency of processing written text. Future research could build on the current work to explore the extent to which ease/difficulty must be consciously considered as opposed to implicitly felt and whether that ease/difficulty must be attributed to privacy management, specifically, or can be a more general perception of ease/difficulty. Similarly, while direct manipulation of the proposed underlying mechanism replicated and reversed effects in a predictable manner for the company control condition in the final study, effects were weaker and reversed for the self control condition. Future research could explore the extent to which the effects herein are driven by differences in privacy's importance as a function of an external source of control, which would map onto the lack of movement seen for the self condition in the first study and some measures for self in the final study. The results suggest greater nuance that is certainly worth exploring.

The studies herein also suggest that perceived privacy importance predicts an individual's willingness to disclosure more private, but not necessarily more anodyne or innocuous

information. The 27 items included in the current studies were inspired by prior research (Lo 2010), were pretested with a sample selected from the same population as the experiments, and assessed in a factor analysis involving over 2,000 participants. However, different content not included could be considered more or less private than the 27 factors included here, not to mention the fact that what is deemed more intimate or sensitive could differ for other groups of individuals. Young people who grew up with social media and technology may assess content differently than older generations who did not. Future work could explore different consumer segments whose perceptions vary in this regard. Similarly, Lo (2010) found relationships among similar kinds of disclosure items (e.g., "somewhat identifying information," "personal contact information," etc.). Future work could test whether the effects herein apply more to particular types or groups of related items beyond the public/private distinction.

Beyond factors specific to individuals, the almost daily reports of privacy breaches and scandals—from Facebook's Cambridge Analytica user privacy controversy to the Equifax data breach—could influence the subjective importance of privacy for society at large. Future research could explore users' willingness to share information before and after these newsworthy events particularly across social networks that differ in the degree to which they claim control over managing privacy. Similarly, future research could explore the ways in which technology companies subtly encourage users to disclose information via design, such as so-called "dark patterns" (ForbrukerRadet 2018), and how these built-in design attributes potentially influence the subjective importance of privacy without users' awareness of this subtle influence.

REFERENCES

Acquisti, Alessandro, and Jens Grossklags (2005), "Privacy and Rationality in Individual Decision Making," *Security and Privacy*, 3 (1), 26–33.

Acquisti, Alessandro, Leslie K. John, and George Loewenstein (2012), "The Impact of Relative Standards on the Propensity to Disclose," *Journal of Marketing Research*, 49 (2), 160–74.

Alashoor, Tawfiq, and Richard Baskerville (2015), "The Privacy Paradox: The Role of Cognitive Absorption in the Social Networking Activity," paper presented at the Thirty Sixth International Conference on Information Systems, Fort Worth, TX.

Alter, Adam L., and Daniel M. Oppenheimer (2009), "Uniting the Tribes of Fluency to Form a Metacognitive Nation," *Personality and Social Psychology Review*, 13 (3), 219–35.

Alter, Adam L., Daniel M. Oppenheimer, Nicholas Epley, and Rebecca N. Eyre (2007), "Overcoming Intuition: Metacognitive Difficulty Activates Analytic Reasoning," *Journal of Experimental Psychology: General*, 136 (4), 569–76.

Barnes, Susan B. (2006), "A Privacy Paradox: Social Networking in the United States," *First Monday*, 11 (9), http://firstmonday.org/article/view/1394/1312.

Barth, Susanne, and Menno D. T. de Jong (2017), "The Privacy Paradox: Investigating Discrepancies between Expressed Privacy Concerns and Actual Online Behavior—a Systematic Literature Review," *Telematics and Informatics*, 34 (7), 1038–58.

Caudill, Eve M., and Patrick E. Murphy (2000), "Consumer Online Privacy: Legal and Ethical Issues," *Journal of Public Policy and Marketing*, 19 (1), 7–19.

Charness, Gary (2000), "Responsibility and Effort in an Experimental Labor Market," *Journal of Economic Behavior and Organization*, 42 (3), 375–84.

Chen, Gilad, Stanley M. Gully, and Dov Eden (2001), "Validation of a New General Self-Efficacy Scale," *Organizational Research Methods*, 4 (1), 62–83.

Choi, Hanbyul, Jonghwa Park, and Yoonhyuk Jung (2018), "The Role of Privacy Fatigue in Online Privacy Behavior," *Computers in Human Behavior*, 81 (April), 42–51.

Citron, Danielle Keats (2017), "The Privacy Policymaking of State Attorneys-General," *Notre Dame Law Review*, 92 (2), 747–816.

——— (2019), "Sexual Privacy," *Yale Law Journal*, 128, 1870–960.

Cohen, Julie E. (2019), *Between Truth and Power: Legal Constructions of Informational Capitalism*, New York: Oxford University Press.

Diemand-Yauman, Connor, Daniel M. Oppenheimer, and Erikka B. Vaughan (2011), "Fortune Favors the Bold and the Italicized: Effects of Disfluency on Educational Outcomes," *Cognition*, 118 (1), 111–15.

DuCette, Joseph, and Stephen Wolk (1972), "Locus of Control and Extreme Behavior," *Journal of Consulting and Clinical Psychology*, 39 (2), 253–58.

Dwyer, Catherine, Starr Roxanne Hiltz, and Katia Passerini (2007), "Trust and Privacy Concern within Social Networking Sites: A Comparison of Facebook and Myspace," paper presented at the Thirteenth Americas Conference on Information Systems, Keystone, CO.

Emerson, Richard M. (1962), "Power-Dependence Relations," *American Sociological Review*, 27 (1), 31–40.

Fogel, Joshua, and Elham Nehmad (2009), "Internet Social Network Communities: Risk Taking, Trust, and Privacy Concerns," *Computers in Human Behavior*, 25 (1), 153–60.

ForbrukerRadet (2018), "Deceived by Design: How Tech Companies Use Dark Patterns to Discourage Us from Exercising Our Rights to Privacy," https://fil.forbrukerradet.no/wp-content/uploads/2018/06/2018-06-27-deceived-by-design-final.pdf.

Fried, Charles (1968), "Privacy," *Yale Law Journal*, 77 (3), 475–93.

Gerber, Nina, Paul Gerber, and Melanie Volkamer (2018), "Explaining the Privacy Paradox: A Systematic Review of Literature Investigating Privacy Attitude and Behavior," *Computers and Security*, 77 (August), 226–61.

Goffman, Erving (1959), *The Presentation of Self in Everyday Life*, New York: Vintage Books.

Haddock, Geoffrey, Alexander J. Rothman, Rolf Reber, and Norbert Schwarz (1999), "Forming Judgments of Attitude Certainty, Intensity, and Importance: The Role of Subjective Experiences," *Personality and Social Psychology Bulletin*, 25 (7), 771–82.

Hargittai, Eszter, and Alice Marwick (2016), "What Can I Really Do? Explaining the Privacy Paradox with Online Apathy," *International Journal of Communication*, 10 (January), 3737–57.

Hartzog, Woodrow (2018), *Privacy's Blueprint: The Battle to Control the Design of New Technologies*, Cambridge, MA: Harvard University Press.

Hartzog, Woodrow, and Evan Selinger (2015), "Surveillance as Loss of Obscurity," *Washington and Lee Law Review*, 72 (3), 1343–87.

Hayes, Andrew F. (2017), *An Introduction to Mediation, Moderation, and Conditional Process Analysis: A Regression-Based Approach*, 2nd ed., New York: Guilford.

Hernandez, Ivan, and Jesse Lee Preston (2013), "Disfluency Disrupts the Confirmation Bias," *Journal of Experimental Social Psychology*, 49 (1), 178–82.

Hoffman, Christian Pieter, Christoph Lutz, and Giulia Ranzini (2016), "Privacy Cynicism: A New Approach to the Privacy Paradox," *Cyberpsychology: Journal of Psychosocial Research on Cyberspace*, 10 (4), article 7.

Hunt, Chris (2011), "Conceptualizing Privacy and Elucidating its Importance: Foundational Considerations for the Development of Canada's Fledgling Privacy Tort," *Queen's Law Journal*, 37 (1), 167–202.

Inness, Julie (1992), *Privacy, Intimacy, and Isolation*, New York: Oxford University Press.

John, Leslie K., Alessandro Acquisti, and George Loewenstein (2011), "Strangers on a Plane: Context-Dependent Willingness to Divulge Sensitive Information," *Journal of Consumer Research*, 37 (5), 858–73.

Li, Han, Rathindra Sarathy, and Heng Xu (2010), "Understanding Situational Online Information Disclosure as a Privacy Calculus," *Journal of Computer Information Systems*, 51 (1), 62–71.

Li, Han, Rathindra Sarathy, and Jie Zhang (2008), "The Role of Emotions in Shaping Consumers' Privacy Beliefs about Unfamiliar Online Vendors," *Journal of Information Privacy and Security*, 4 (3), 36–62.

Lo, Janice (2010), "Privacy Concern, Locus of Control, and Salience in a Trust-Risk Model of Information Disclosure on Social Networking Sites," in *Proceedings of the Sixteenth Americas Conference on Information Systems*, Red Hook, NY: Curran, 110–12.

Lwin, May, Jochen Wirtz, and Jerome D. Williams (2007), "Consumer Online Privacy Concerns and Responses: A Power-Responsibility Equilibrium Perspective," *Journal of the Academy of Marketing Science*, 35 (4), 572–85.

Madden, Mary, and Lee Raine (2015), *Americans' Attitudes about Privacy, Security, and Surveillance*, Washington, DC: Pew Research Center.

Mathur, Arunesh, Gunes Acar, Michael J. Friedman, Elena Lucherini, Jonathan Mayer, Mershini Chetty, and Arvind Narayanan (2019), "Dark Patterns at Scale: Findings From a Crawl of 11K Shopping Websites," in *Proceedings of the ACM Human-Computer Interactions*, Vol. 3, New York: Association for Computing Machinery, article 81, 1–32.

Mourey, James A., Ben C. P. Lam, and Daphna Oyserman (2015), "Consequences of Cultural Fluency," *Social Cognition*, 33 (4), 308–44.

Murphy, Patrick E., Gene R., Laczniak, Norman E. Bowie, and Thomas A. Klein (2005), *Ethical Marketing: Basic Ethics in Action*, Upper Saddle River, NJ: Prentice-Hall.

Nissenbaum, Helen (2004), "Privacy as Contextual Integrity," *Washington Law Review*, 79 (1), 119–57.

——— (2009), *Privacy in Context: Technology, Policy, and the Integrity of Social Life*, Palo Alto, CA: Stanford University Press.

Norberg, Patricia A., Daniel R. Horne, and David A. Horne (2007), "The Privacy Paradox: Personal Information Disclosure Intentions Versus Behaviors," *Journal of Consumer Affairs*, 41 (1), 100–126.

Oyserman, Daphna, Kristen Elmore, Sheida Novin, Oliver Fisher, and George C. Smith (2018), "Guiding People to Interpret their Experienced Difficulty as Importance Highlights Their Academic Possibilities and Improves Their Academic Performance," *Frontiers in Psychology*, 9 (May), 781–96.

Pasquale, Frank (2015), *Black Box Society: The Secret Algorithms That Control Money and Information*, Cambridge, MA: Harvard University Press.

Pocheptsova, Anastasiya, Aparna A. Labroo, and Ravi Dhar (2010), "Making Products Feel Special: When Metacognitive Difficulty Enhances Evaluation," *Journal of Marketing Research*, 46 (6), 1059–69.

Posner, Richard A. (1978a), "The Right of Privacy," *Georgia Law Review*, 12 (3), 393–422.

——— (1978b), "An Economic Theory of Privacy," *Regulation*, 2 (3), 19–26.

Post, Robert (1989), "The Social Foundations of Privacy: Community and Self in the Common Law Tort," *California Law Review*, 77 (5), 957–1010.

Reidenberg, Joel R., Travis Breaux, Lorie F. Cranor, and Brian French (2015), "Disagreeable Privacy Policies: Mismatches between Meaning and Users' Understanding," *Berkeley Technology Law Journal*, 30 (1), 39–68.

Reidenberg, Joel R., N. Cameron Russell, Alexander Callen, Sophia Qasir, and Thomas Norton (2014), "Privacy Harms and the Effectiveness of the Notice and Choice Framework," *I/S: A Journal of Law and Policy for the Information Society*, 11 (2), 485–524.

Reynolds, Douglas B., Jacob Joseph, and Reuben Sherwood (2009), "Risky Shift versus Cautious Shift: Determining a Dichotomy between Private and Public Investment Decision-Making," *Journal of Business and Economics Research*, 7 (1), 63–78.

Savary, Jennifer, and Ravi Dhar (2014), "When Quitting Feels Like Giving Up: Self-Signaling in Retention Choice," https://ssrn.com/abstract=3077374.

Scheibehenne, Benjamin, Rainer Greifender, and Peter M. Todd (2010), "Can There Ever Be Too Many Options? A Meta-Analytic Review of Choice Overload," *Journal of Consumer Research*, 37 (3), 409–25.

Schwarz, Norbert (2011), "Feelings-as-Information Theory," in *Handbook of Theories of Social Psychology*, Vol. 1, ed. Paul A. M. Van Lange, Arie W. Kruglanski, and E. Tory Higgins, Newbury Park, CA: SAGE, 289–308.

Solove, Daniel J. (2008), *Understanding Privacy*, Cambridge, MA: Harvard University Press.

Solove, Daniel J., and Woodrow Hartzog (2014), "The FTC and the New Common Law of Privacy," *Columbia Law Review*, 114 (2), 583–676.

Song, Hyunjin, and Norbert Schwarz (2009), "If It's Difficult to Pronounce, It Must Be Risky: Fluency, Familiarity, and Risk Perception," *Psychological Science*, 20 (2), 135–38.

Stigler, George J. (1980), "An Introduction to Privacy in Economics and Politics," *Journal of Legal Studies*, 9 (4), 623–44.

Turow, Joseph, Michael Hennessy, and Nora Draper (2015), *The Tradeoff Fallacy: How Marketers Are Misrepresenting American Consumers and Opening Them Up to Exploitation*, Philadelphia: Annenberg School for Communication.

Veltri, Guiseppe A., and Andriy Ivchenko (2017), "The Impact of Different Forms of Cognitive Scarcity on Online Privacy Disclosure," *Computers in Human Behavior*, 73 (August), 238–46.

Waldman, Ari Ezra (2018), *Privacy as Trust: Information Privacy for an Information Age*, New York: Cambridge University Press.

Westin, Alan F. (1968), "Privacy and Freedom," *Washington and Lee Law Review*, 25 (1), 166–70.

——— (1997), "Whatever Works: The American Public's Attitudes toward Regulation and Self-Regulation on Consumer Privacy Issues," in *Privacy and Self-Regulation in the Information Age*, Washington, DC: National Telecommunications and Information Administration, https://www.ntia.doc.gov/page/chapter-1-theory-markets-and-privacy.

White, Tiffany Barnett (2004), "Consumer Disclosure and Disclosure Avoidance: A Motivational Framework," *Journal of Consumer Psychology*, 14 (1–2), 41–51.

——— (2005), "Consumer Trust and Advice Acceptance: The Moderating Roles of Benevolence, Expertise, and Negative Emotions," *Journal of Consumer Psychology*, 15 (2), 141–48.

Zuboff, Shohana (2019), *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*, New York: Public Affairs.