When Disclosure is Involuntary: Empowering Users with Control to Reduce Concerns

Completed Research Paper

David W. Wilson
University of Oklahoma
Norman, Oklahoma
davidwilsonphd@gmail.com

Ryan M. Schuetzler
University of Nebraska at Omaha
Omaha, Nebraska
ryan@schuetzler.net

Bradley Dorn
University of Arizona
Tucson, Arizona
bdorn@email.arizona.edu

Jeffrey G. Proudfoot
Bentley University
Waltham, Massachusetts
jproudfoot@bentley.edu

Joseph S. Valacich
University of Arizona
Tucson, Arizona
jsvalacich@cmi.arizona.edu

Abstract

Modern organizations must carefully balance the practice of gathering large amounts of valuable data from individuals with the associated ethical considerations and potential negative public image inherent in breaches of privacy. As it becomes increasingly commonplace for many types of information to be collected without individuals' knowledge or consent, managers and researchers alike can benefit from understanding how individuals react to such involuntary disclosures and how these reactions can impact evaluations of the data-collecting organizations. This research develops and empirically tests a theoretical model that shows how empowering individuals with a sense of control over their personal information can help mitigate privacy concerns following an invasion of privacy. Using a controlled experiment with 94 participants, we show that increasing control can reduce privacy concerns and significantly influence individuals' attitudes toward the organization that has committed a privacy invasion. We discuss theoretical and practical implications of our work.

Keywords: privacy, involuntary disclosure, perceived control

Introduction

In December 2009, following a steady stream of high-profile privacy incidents from large companies (e.g., Yahoo, Verizon, and Sprint), Google CEO Eric Schmidt was asked a pointed question regarding Google's expansive data collection practices. Echoing the opinions of a large number of Americans, a reporter suggested that Google was collecting and storing private information that many people only shared with their most trusted friends. Rather than reassuring the reporter—and the listening audience—that Google's practices were safe, beneficial, or otherwise justified, Schmidt responded that "if you have something that you don't

want anyone to know, maybe you shouldn't be doing it in the first place" (Tate 2009). Schmidt's tone-deaf response incited substantial criticism of the company's dismissive stance toward individuals' privacy, and has contributed to a general trend of public caution toward interacting with Google's many online services (Adams 2012).

Though this anecdote involving Google provides an opportunistic example, it is increasingly common for companies to engage in large-scale capture, storage, and analysis of Internet users' personal information (Vaidhyanathan 2011). These large sets of data are not all bad; among other things, the advertising revenue generated through leveraging troves of (mostly anonymous) data allows companies like Google and Facebook to offer their popular services to the public free of charge. Users of the Android phone operating system further benefit from this data collection, as Google is able to offer personalized recommendations and information, including weather forecasts, traffic reports, and appointment reminders. Additionally, many companies derive significant business value from these data, enabling new and interesting business models such as the recent expansion of *big data* analysis (McKinsey Global Institute 2011).

However, these economic advances come at a cost. Such widespread collection of personal and behavioral information generates significant trepidation by the general public (Burst Media 2009; UK Information Commissioner's Office 2013), and negative opinions regarding information-gathering activities are detrimental to a company's image (Best 2014; Herold 2014). The data being collected are increasingly positioned as a *condition of use* of many online services (Son and Kim 2008), and even concerted efforts to shield one's personal information from the many data repositories are ineffective and cost-prohibitive to pursue (Vertesi 2014). With elevated public concern about privacy, well-meaning organizations are faced with limited options: (1) cease collecting certain information, (2) collect information in secret, or (3) assuage user concern regarding the information that is collected. The first choice is a non-option for most online companies, and many pursue a combination of the second and third choices by suppressing publicity regarding how much data is being collected and engaging with the public to reduce concerns (Johnson 2010).

In response to these pressing issues, this research investigates how organizations can relieve users' *information privacy concerns* (IPC) regarding personal information that has already been (involuntarily) collected (i.e., informing the third strategy in the list above). *Involuntary disclosure* is here defined as information collected by an organization without the informed consent of the individual. Very often today we see long terms of service and privacy policies, and users are inclined to click through without reading or understanding the policies they are agreeing to. Even operating systems like Windows 10 include data-collecting software that users may view as a violation of their privacy (Forrest 2015). This study addresses how an organization can address user privacy concerns after data has been collected. In doing so, we contribute uniquely to the privacy literature—which has been limited in addressing this type of disclosure—and provide important managerial guidance to aid organizations seeking to find effective ways to balance users' privacy considerations with the value (or, in come cases, necessity) of personal information collected about individuals. Information privacy concerns are generally defined as an individual's concerns about possible loss of privacy (Smith et al. 2011). Given the difficulty of measuring the concept of privacy itself, IPC has been the measurement proxy of choice for nearly all prior information privacy research (Smith et al. 2011). As such, IPC has received extensive theoretical and empirical treatment in the IS literature (e.g., Dinev and Hart 2006; Hong and Thong 2013; Malhotra et al. 2004; Smith et al. 1996; Xu et al. 2011), most of which has framed IPC as a primary obstacle to overcome for personal information disclosure or other online interactions to take place.

Our contribution to the privacy literature is significant for at least two reasons. First, we know relatively little about the determinants of IPC in general, as most prior research has employed IPC as a predictor of other privacy-related outcomes (Smith et al. 2011). Second, what little literature exists investigating the determinants of IPC has been based solely in e-commerce or mobile commerce settings (Xu 2007; Xu et al. 2011; Xu and Teo 2004; Xu et al. 2012), where the ultimate goal in measuring IPC is to predict users' disclosure decisions. However, traditional models of disclosure may not be adequate to explain IPC reduction in an involuntary disclosure context in which disclosure has already occurred.

To overcome these potential inadequacies in prior literature, the research model developed here focuses on determinants of IPC in involuntary disclosure situations. The model employs the perceived control con-

struct as a key determinant of IPC, following prior research (Xu 2007; Xu et al. 2011; Xu and Teo 2004; Xu et al. 2012). Two characteristics distinguish this model from prior literature and tailor it to the involuntary disclosure context. First, two key predictors of perceived control are adapted from the psychological stress literature (Averill 1973), namely behavioral control—the feeling that one can influence or modify the nature of a threatening event—and cognitive control—the feeling that one understands the nature of a threatening event. These types of control contribute to one's perceived control and are useful for their ease of implementation, as discussed below. Second, the model replaces disclosure behavior with an evaluation of participants' attitudes regarding the company as the ultimate dependent variable. The result is a model particularly suited to a case where disclosure occurs and the goal is to reduce resulting concerns and maintain positive evaluations of the information-collecting organization without changing this disclosure.

Related Literature

Before building the theoretical model, we first provide some background for the theory and concepts used within the model. We review the privacy literature to establish privacy as a form of control over personal information, and to explore prior work that has identified antecedents to IPC. We then provide a brief background in the psychological stress literature to define both behavioral and cognitive control. Finally, we review the literature that has investigated privacy issues in the context of involuntary disclosure.

Control as an Antecedent of Privacy Concerns

Control is found among the earliest conceptualizations of privacy (Altman 1975; Westin 1967)—Altman's (1975) oft-cited definition of privacy is "the selective control of access to the self" (p. 24)—and has persisted as a common concept in nearly every rendition of privacy in the years since. Despite its deep history in the study of privacy, however, control has been treated rather inconsistently in the IS literature. Some researchers consider privacy to be a form of control *per se* (e.g., Altman 1975; Goodwin 1991; Milne and Rohm 2000), while others assume control to be antecedent to privacy (e.g., Dinev and Hart 2004; Laufer and Wolfe 1977). The most common scales used to measure privacy (Hong and Thong 2013; Malhotra et al. 2004; Smith et al. 1996) have included control as one (though not the only) dimension of privacy. As Solove (2002) noted, "[privacy] theorists provide little elaboration as to what control really entails, and it is often understood too narrowly or too broadly" (p. 1112). Margulis argues that there remains an opportunity to further clarify the nature of control in the context of privacy (Margulis 2003a; Margulis 2003b).

While the inconsistency highlighted above may seem disconcerting, the last decade of privacy research in the IS discipline has seen growing consensus that control and privacy should be treated as separate concepts, with control as a predictor of privacy (Smith et al. 2011). Dinev and Hart (2004) argue that "when people have a greater sense that they control the use of their information, they will have fewer privacy concerns" (p. 416). This view has been reinforced by several other studies in which perceived control is a significant predictor of privacy concerns (e.g., Hoadley et al. 2009; Xu 2007). Most recently, Xu et al. (2012) offered strong theoretical clarification and empirical evidence regarding the role of perceived control as a mediator of privacy concerns. Their study adopted control agency theory to distinguish between personal control—which empowers an individual with personal control over their privacy—and proxy control—in which third parties such as government or industry regulators act as control agents to protect privacy. Their findings support the notion that perceived control, derived from both personal and proxy control, plays an important, mediating role in determining privacy concerns.

This relatively small core of literature investigating control as a predictor of privacy concerns is valuable for another reason. Even as IPC has become the most common conceptualization of, and measurement proxy for, privacy, we know relatively little regarding the factors that determine an individual's IPC. In their extensive review of the privacy literature, Smith et al. (2011) note that only a minority of privacy research has explored the determinants of IPC, with most theorists opting instead to explore the outcomes of individuals' IPC. Those studies that have examined the formation of IPC have identified prior privacy invasions (Smith et al. 1996), general awareness of privacy practices (Malhotra et al. 2004), and personality (Bansal et al. 2010; Lu et al. 2004; Xu 2007) and demographic (Chen and Rea 2004; Culnan and Armstrong 1999; Sheehan 1999; Sheehan and Hoy 2000) differences, among others, as significant predictors. In one particular

stream of research, Xu and colleagues (Xu 2007; Xu et al. 2008; Xu et al. 2011; Xu and Teo 2004; Xu et al. 2012) explored a variety of antecedents to IPC, including dispositional measures, perceived risks, and various forms of institutional assurances. These prior studies constitute an important initial exploration of the antecedents of IPC. However, as Smith et al. (2011) suggest, our understanding of the antecedents of IPC is limited, and there is value in empirical studies that contribute to this area of research.

Following the recent trend in the privacy literature that has separated perceived control as an important antecedent of privacy, and in response to the more general need for greater understanding of the factors that shape IPC, the model developed in this study highlights the important role of control in shaping privacy concerns. We provide a unique perspective on the notion of control, however, given our focus on reducing IPC in the context of involuntary disclosure. In such situations, the privacy invasion has already occurred and our objective is to reduce the negative perceptions related to the invasion. The next section examines the psychological stress literature, which positions control as an effective countermeasure to a negative, stressful event.

Reducing Psychological Stress with Control

Control is deeply important to psychological functionality, and many decades of research have demonstrated that a sense of control is a consistent predictor of physical and mental well-being (Skinner 1996). Among its many virtues, control has long been accepted as an effective countermeasure to stressful and negative (even painful) stimuli (Averill 1973; Carlsson et al. 2006; Müller 2011; Salomons et al. 2004). In short, "personal control makes it possible to incorporate a potentially threatening event into a cognitive plan, thus reducing anxiety" (Averill 1973, p. 286).

Our focus is on reducing the negative effects of a privacy invasion that has already occurred. To understand the effect of control in soothing individuals' concerns about their privacy after such an invasion, we draw from the psychological stress literature, which provides two helpful forms of control that serve to ease an individual's anxiety—behavioral control and cognitive control. We propose that manipulating these two forms of control will reduce anxiety resulting from privacy concerns after a disclosure has occurred.

Behavioral control is one's perception that a direct, behavioral response is available that can affect, alter, or even terminate a negative event (Averill 1973). This type of control empowers an individual with a feeling that he or she can direct the outcome of a stressful situation, thereby reducing uncertainty and perceived risk related to the negative event. Interestingly, people desire control over a negative stimulus even when that control does not actually alter the nature of the threat (Staub et al. 1971). For example, participants in one study reported significantly lower perceived pain after they themselves administered an electric shock compared to participants for whom an experimenter administered the shock, even though the intensity of the electric shock was the same for both groups (Müller 2011). This phenomenon is particularly relevant for our involuntary disclosure context, in which the stressful event (i.e., the privacy invasion) has already occurred. Individuals in this situation are not able to prevent the past disclosure, but through other means of promoting behavioral control, it may be possible to effect an anxiety-reducing outcome. Our theoretical model and experimental procedures will explore this possibility.

Cognitive control refers to the way in which an event is interpreted, understood, and appraised (Averill 1973). It has been shown that pain, discomfort, or stress can be mitigated on the basis of a person's interpretation of events (Averill 1973). In one study, for example, researchers manipulated cognitive control among patients about to undergo major surgery by providing detailed information on the surgery procedures and calming the patient's fears regarding the potential pain and discomfort expected during recovery (Langer et al. 1975). This manipulation reduced pre- and postoperative stress, and patients in this treatment group requested significantly fewer pain relievers following surgery and went home sooner than other patients. Cognitive control has also been found to reduce uncertainty and increase satisfaction in customer service engagements (Faranda 2001; Namasivayam 2004) and to play a key role in reducing workplace stress and increasing job satisfaction among employees (Fila et al. 2014; Ganster 1989). Thus, increasing an individual's understanding of a given negative event (e.g., an involuntary disclosure) can significantly reduce the pain and stress incurred by the event. Importantly, this reduction in anxiety occurs without actually modifying the negative event.

In summary, the psychological stress literature provides two unique methods of producing perceived control when a negative event is considered inevitable or unavoidable. Thus, behavioral and cognitive control constitute plausible mechanisms through which perceived control can be produced. Our experimental design will specifically explore such mechanisms in the context of an involuntary disclosure. Before building our model, however, we first review the relatively small set of prior work that has investigated privacy concerns in involuntary situations.

Prior Studies Investigating Privacy in the Context of Involuntary Disclosure

As a condition of usage, most online services require their users to provide varying levels of personal information. Though this does not constitute strict involuntary disclosure (since individuals can choose to simply not use these services), individuals who choose to use the Internet are forced to disclose at least some amount of private information. Despite this fact, the vast majority of disclosure-related privacy research has focused on individuals' *choices* regarding whether to disclose information. These prior investigations usually measure individuals' willingness or intentions to disclose personal information (e.g., Dinev et al. 2006; Dinev and Hart 2006; Li et al. 2010; Malhotra et al. 2004; Xu et al. 2009), with a more limited subset having studied actual disclosure behavior (e.g., Keith et al. 2013; Norberg 2007). Studies that follow this disclosure-decision paradigm have been extremely valuable, but have always carried the assumption that the user has not yet disclosed any information. Relatively little research has examined privacy issues under the general assumption that disclosure has already occurred.

However, some prior work has examined nonconsensual monitoring of computer or Internet behavior, usually referred to as surveillance. This research has examined the privacy-related implications of governmental surveillance (Dinev et al. 2008), organizational surveillance of employees' computer behavior (e.g., Alge 2001), as well as the issues surrounding the tracking of online browsing behavior via browser cookies by online companies (e.g., Cranor et al. 2006; Martin et al. 2003; Milne et al. 2004; Miyazaki 2012; Sheehan 2005). An interesting commonality among these streams of surveillance research is found in the effect of transparency in reducing privacy concerns. Employees who are told they are being surveilled (Alge 2001) and Internet users who are informed of websites' cookie monitoring procedures (Miyazaki 2012) report fewer concerns about their privacy. Furthermore, citizens who perceive a legitimate need for government surveillance report being less concerned about their private information being potentially accessed by government agencies (Dinev et al. 2008). These prior findings relate well to the concept of cognitive control developed within our model. Our model develops this concept further into an explicit driver of perceived control intended to assuage user concern about the private information that has already been disclosed.

In summary, though privacy theorists have long considered control to be an integral part of privacy, there remains ambiguity in the literature regarding the role of control in shaping IPC. Given our unique, involuntary disclosure context, the psychological stress literature provides two promising mechanisms that may help users feel that they have greater control over the aftermath of a privacy-threatening disclosure. Furthermore, while a great deal of prior research has helped us understand the factors that influence users' disclosure decisions, relatively little has studied privacy issues in situations where the disclosure has already happened. We thus develop a research model and propose specific hypotheses in the next section to explain how users' privacy concerns about involuntarily disclosed information can be mitigated through control-enhancing interventions.

Theory Development and Research Model

Our research model, shown in Figure 1, comprises a set of hypotheses that summarize the factors that shape privacy concerns in the involuntary disclosure context. We first discuss dispositional factors that influence perceived control and IPC. We then leverage the psychological stress literature to justify hypotheses relating behavioral and cognitive control to perceived control. Finally, we argue for beneficial effects of perceived control on users' attitudes toward the data-collecting organization, partially mediated by the user's IPC. The resulting research model provides a unique description of how privacy concerns are formed when an involuntary disclosure has occurred, and how those concerns and associated attitudinal assessments can be managed by applying control-related interventions.

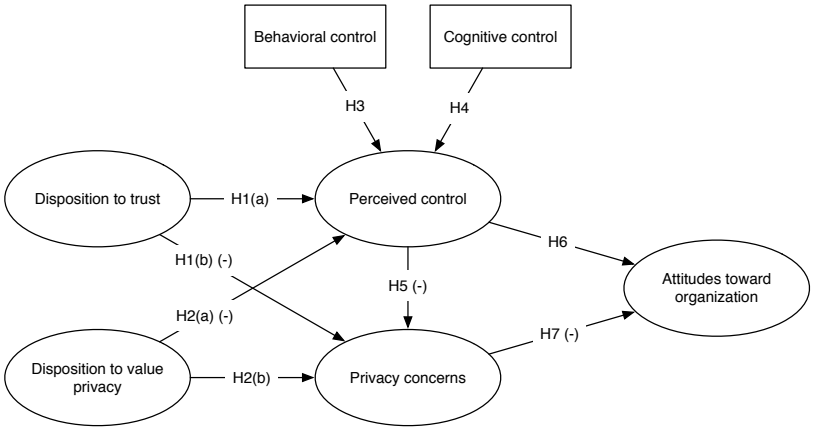

Figure 1. Research Model with Hypotheses

Dispositional Characteristics

Individuals vary in the extent to which they value privacy and are willing to submit themselves to potentially risky situations. These differences are likely the result of a wide range of factors, including an individual's past experiences, personality traits, cultural beliefs, and so on. These dispositional factors significantly impact users' decisions, particularly when the user is interacting with unfamiliar transaction partners (Mayer et al. 1995; McKnight et al. 1998; Rotter 1971). While the impact of dispositional factors has long been accepted in the context of trusting relationships (Colquitt et al. 2007), they have received substantially less attention from privacy theorists. (Exceptions include Li 2011; Li 2014a; Morton n.d.; Patil and Kobsa 2005; Phelps et al. 2001; Rensel et al. 2006; Richards 2012; Xu et al. 2008; Xu et al. 2011; Yao and Zhang 2008). We identify two different dispositional factors that will help predict the control and privacy concepts within our model—disposition to trust and disposition to value privacy.

An individual's *disposition to trust* is a personality-based trait summarizing a person's general willingness to trust others (Mayer et al. 1995). Trust has been shown to play an important role in many prior privacy studies (e.g., Bélanger et al. 2002; Dinev et al. 2006; Dinev and Hart 2006), but the role of an individual's disposition to trust in determining privacy-related outcomes has not been extensively studied. In order to connect dispositional trust to privacy outcomes, we first consider that a key function of trust is to reduce uncertainty in a given transaction (Metzger 2004). If individuals are generally more trusting, then, they should feel considerably less uncertainty and, by extension, be more likely to feel a sense of control in the context of an online interaction. Prior research has provided some evidence for a link between trust and control (Arcand et al. 2007; Walczuch and Lundgren 2004), though the relationship is somewhat tenuous, having been infrequently tested. In an exploratory effort to better understand the effect of this dispositional factor within our context, we hypothesize that an individual's disposition to trust will have a facilitating role in the formation of IPC. We further assume that this facilitating role will be partially mediated through perceived control, such that disposition to trust will both positively impact perceived control and negatively impact IPC. Thus, we hypothesize:

> *H1: An individual's disposition to trust will (a) positively influence the individual's perceived control and (b) negatively influence the individual's privacy concerns.*

In contrast to the rather under-studied trait of disposition to trust (in the context of privacy), dispositional factors related to an individual's need for or tendency to value personal privacy have been more popular among privacy researchers. *Disposition to value privacy* is a personality attribute reflecting an individual's inherent need to maintain certain boundaries that frame personal information space, and is defined as "an individual's general tendency to preserve his or her private information space or to restrain disclosure of personal information across a broad spectrum of situations and contexts" (Xu et al. 2011, p. 805). One's disposition to value privacy has been found to positively influence an individual's privacy concerns, given

that those who inherently value their privacy will desire more control over the disclosed information, and thus generally be more concerned about any information that has been disclosed (Li 2011; Li 2014a; Morton n.d.; Patil and Kobsa 2005; Phelps et al. 2001; Rensel et al. 2006; Richards 2012; Xu et al. 2008; Xu et al. 2011; Yao and Zhang 2008). We thus hypothesize a positive relationship between an individual's disposition to value privacy and his or her level of IPC. In addition, an individual who naturally assigns a higher value to privacy will perceive a given invasion of privacy as more intrusive and the feeling that control has been lost will be magnified. Thus we additionally hypothesize a negative impact of disposition to value privacy on perceived control, following prior literature (Xu et al. 2008; Xu et al. 2011). In summary, we hypothesize:

> *H2: An individual's disposition to value privacy will (a) negatively influence the individual's perceived control and (b) positively influence the individual's privacy concerns.*

The Role of Control in Shaping Privacy Concerns

Nearly every academic conversation on the topic of privacy includes the concept of control in some form (Altman 1975; Smith et al. 2011; Westin 1967; Xu et al. 2012). Our model embraces this trend and focuses directly on the role of control in reducing IPC and improving users' evaluations of the data-collecting organization. We instantiate this control as *perceived control*, which is defined as "an individual's belief about the presence of factors that may increase or decrease the amount of control over the release and dissemination of personal information" (Xu et al. 2012, p. 5). Aside from the dispositional factors already discussed, we argue that perceived control can be significantly improved by providing users the two forms of control we have derived from the psychological stress literature (Averill 1973)—behavioral control and cognitive control.

Behavioral control refers to the perception that a direct, behavioral response is available that can affect, alter, or even terminate a negative event (Averill 1973). Behavioral control empowers an individual with the feeling that he or she "has a say" in what will happen in a given situation. Though this concept has applications in a wide variety of contexts, we focus on the outcomes of behavioral control in a situation where a negative, stressful event, such as a privacy-invading disclosure, has occurred.

When an individual is faced with an anxiety-inducing event, there are a number of ways in which behavioral control might be granted. The most direct method—and, arguably, the one most effective at reducing anxiety—is to allow the individual to either prevent or reduce the negative impact of the event. In the experimental psychology domain, this form of behavioral control is referred to as stimulus modification (Averill 1973), and has been implemented by allowing participants, for example, to opt-out of receiving an electric shock, to reduce the intensity of the shock, or by having punishment contingent upon the performance of some task (Averill 1973). In the privacy literature, this concept is easily recognized in what have been termed privacy-enhancing technologies (Burkert 1997), or technologies that allow individuals to protect their information privacy by directly controlling the flow of their personal information to others (Xu et al. 2012). Examples of such technologies include the privacy controls provided to users of online social networks (Hoadley et al. 2009) or automated web browser tools for reading and evaluating website privacy policies (Cranor et al. 2006). In addition to these privacy-enhancing technologies, Internet users worried about their privacy sometimes have the ability to either falsify the personal information they provide or avoid disclosure altogether (Son and Kim 2008).

While the actions listed above can be effective in producing control and reducing privacy concerns, we categorically exclude these types of control-enhancing factors from our investigation. We focus instead on situations where disclosure has already taken place or is mandatory as a condition of use, and we therefore assume that this popular avenue for providing control to the user is not an option. In other words, we focus on what *other* methods organizations can employ in order to increase perceived control and reduce privacy concerns. To this end, we explore methods of effecting behavioral control that do not allow the individual to actually reduce the intensity of the negative event.

Behavioral control can also be generated by empowering an individual with the ability to direct—but not actually modify—the execution of the negative event. This is referred to in the psychology literature as regulated administration (Averill 1973). For example, employees who control the scheduling of distasteful office work are subject to less stress and fatigue than employees who are required to follow a regulated schedule for

the same amount of work (Hockey and Earle 2006). Even something as simple as allowing participants to choose their seats during an anxiety-inducing experiment can reduce reported anxiety (Endler et al. 2001). In the context of privacy and involuntary disclosure, this type of control could be granted to a user by allowing him or her the ability to direct the sharing of personal information with third-party organizations, or by allowing the user to ensure that the information that was disclosed is accurate before it is shared with a third party. We hypothesize that taking such measures to provide behavioral control over his or her private information would increase a user's sense of control over that information, even without actually reducing the user's exposure to privacy-related risks. Thus, we hypothesize:

> *H3: Providing an individual behavioral control over his/her personal information will positively influence the individual's perceived control.*

Cognitive control refers to the way in which an event is interpreted, understood, and appraised (Averill 1973). The psychology and management literatures have produced many examples in which pain or stress is reduced simply by helping an individual better understand the nature of a negative event (Averill 1973; Langer et al. 1975). Again, we note that these effects have been observed when the occurrence and intensity of the negative event is not modified, which aligns well with our involuntary disclosure context. If personal information has already been disclosed, cognitive control could be granted to users by clearly explaining and/or justifying the organization's need for the disclosed information, or by clearly explaining the extent of disclosure (i.e., exactly what has been disclosed). We observe similar effects of transparency in situations of surveillance or Internet tracking (Alge 2001; Dinev et al. 2008; Miyazaki 2012), in which concerns have been reduced. According to our theory, this reduction in privacy concerns observed in prior literature is the result of increases in cognitive control, which serve to increase the individual's overall perceived control. In summary, we hypothesize:

> *H4: Providing an individual cognitive control over his/her personal information will positively influence the individual's perceived control.*

A consistent theme in prior privacy research is that consumers tend to have fewer privacy concerns when they believe that they have control over their personal information (Culnan and Armstrong 1999; Culnan and Bies 2003; Phelps et al. 2001; Xu et al. 2011; Xu et al. 2012). Given that one's concerns about privacy are, to an extent, generated by a feeling that one has lost the ability to decide who has access to their personal information (Hong and Thong 2013), this inverse control-concern relationship is quite logical and certainly not unique to our study. We therefore follow prior literature and predict that increasing perceived control will reduce individuals' IPC. Thus we hypothesize:

> *H5: Increasing an individual's perceived control will negatively influence the individual's privacy concerns.*

Linking Privacy Issues to Organizational Evaluations

Negative opinions regarding information-gathering activities are detrimental to an organization's image (Best 2014; Herold 2014), and there is evidence that companies that take measures to protect the privacy of their customers may gain a competitive advantage over their less privacy-conscious competitors (Tsai et al. 2011). We argue that in addition to these prior findings that customers are willing to pay a premium to privacy-conscious companies, such companies will also earn greater respect and affective judgments by embracing positive privacy practices. In other words, companies who respect their customers' privacy can expect their customers to have more positive attitudes towards the company. Given our focus on control as a central driver of privacy-related outcomes, we argue further that increasing users' perceived control will positively impact those users' *attitudes towards the data-collecting organization*. Prior research has shown that individuals' attitudes can be affected by their perceived control over their behavior (Bandura 1991) and this sense of control can impact both intentions and attitudes (Dzewaltowski et al. 1990). We find further

support for this notion in prior marketing research (Tucker 2014), in which online social network users provided with privacy controls were significantly more likely to click on advertisements by third parties, even when these advertisements used personalized text derived from private information. Tucker (2014) speculates that part of this increase in successful advertising was the result of more positive evaluation of the online social network that collected the personal information. Building on this prior literature, we specifically link the increases in perceived control with a user's attitudes toward the organization collecting the data, and we hypothesize:

> *H6: Increasing an individual's perceived control will positively influence the individual's attitudes toward the organization.*

While increasing perceived control will have a positive impact on attitudes, this effect is likely to be largely mediated by the user's IPC. Privacy concerns have long been studied as a predictor of user attitudes in various forms (Culnan 1993; Smith et al. 1996). As Angst and Agarwal (2009) note in the context of IPC, "individuals who harbor strong concerns about a particular issue require particularly compelling arguments to modify their belief structure" (p. 349). A trend of the majority of this prior literature, however, has focused on attitudes toward a particular practice or activity, e.g., collecting information (Smith et al. 1996), secondary use (Culnan 1993), personalization (Chellappa and Sin 2005), and so on. We break from this tradition and posit a relationship between users' IPC and their affective evaluation of the organization collecting information. We expect this relationship to follow prior findings regarding the link between privacy concerns and other attitudes, namely that higher levels of IPC will be associated with lower attitudinal assessments of the data-collecting organization. Taken together, this prediction, and that indicated by *H5*, comprise a partially mediated effect of perceived control on attitudes toward the organization. In summary, we hypothesize:

> *H7: An individual's privacy concerns will negatively influence the individual's attitudes toward the organization.*

Methodology

Our method entails presenting participants with a description of a company (which participants received as a part of the experimental manipulation, described below) and then asking them to provide an overall opinion of the company on the basis of the information provided. Subjects were recruited from an undergraduate course at a large university in the United States. Student subjects are appropriate for this context, since they are heavy users of the Internet and social media (Jones 2009), where privacy disclosure behaviors are a growing issue (Giles 2010). Student samples are also beneficial for experimental procedures, since they tend to be homogenous and provide maximal control over the experimental manipulations (Dennis and Valacich 2001).

Measurement

All measures were adapted from prior research. Measures for disposition to trust were adapted from (Jarvenpaa et al. 1998) and those for disposition to value privacy from (Xu et al. 2011). IPC was measured using items adapted from (Li 2014b), and items for perceived control were adapted from (Xu et al. 2011). Finally, attitudes toward the organization were measured using the method developed by Brown and Dacin (1997). In addition to the constructs found within our theoretical model, we also included measures of various demographic variables, such as age, sex, and ethnicity, as well as measures of prior privacy invasion experiences and general privacy awareness, as control variables.

Experimental Procedure

The experiment employed a 2 x 2 factorial design in which behavioral control (high/low) was crossed with cognitive control (high/low), following the operationalizations described below. Participants first completed a presurvey in which they consented to participate in the study and provided demographic data and other measures, including those for the dispositional factors in the model. This was completed on the participants'

personal computer via a web-based survey application. They were then told that they would need to complete an in-person task in the lab to receive credit, but that all lab sessions were currently full. In reality there were no lab sessions at all, and this deception was a part of the experimental manipulation. They were informed that they would be contacted by the research team when more slots were made available. After a considerable time (nearly two months), participants received an email stating that the lab portion of the experiment had been cancelled, but that they could complete the second portion of the study via the same online survey system that was used to collect the presurvey information. At the beginning of this second online survey, they learned that a (fictitious) online marketing company had been tracking their online activities since they began their participation nearly two months earlier. They were further told (deceptively) that they had consented to this tracking and data gathering procedure when they agreed to participate in the study. This was intended to simulate a now-common, real-world situation in which a user unknowingly agrees to disclose some personal information by failing to read the fine-print of a privacy policy. The participants learned that their browsing history, including websites visited, search engine queries, videos watched, etc., had all been recorded and would be used by the fictitious marketing company for marketing purposes. They were led to believe that they had already forfeited their right to have that information removed when they agreed to participate in the study. All of these measures were taken in order to effect the perception that the information disclosure had already taken place, and that there was no option for the participant to prevent or cancel the privacy invasion. This provided the unique (but rather realistic) context for our experimental manipulations to take effect, as described below.

Participants were randomly assigned to one of four conditions within our 2 x 2 design. For the low behavioral control condition, participants were told that their browsing profile information would be shared with two different third-party marketing organizations, randomly selected from a list of six possible organizations. Individuals in the high behavioral control condition were allowed to choose exactly two of the six third-party organizations with whom the information would be shared. Participants in the high behavioral control condition were further informed that they would be able to check the data for accuracy and correct any potential errors (though they would not be able to remove the data or prevent it from being shared). They were informed that they would receive a followup email from the fictitious company with instructions regarding this checking procedure. Participants in the low behavioral control condition were not informed of any data-checking procedure. For the cognitive control manipulations, those in the high cognitive control condition were informed that the marketing company sponsoring the research had a strict transparency policy that required them to inform individuals each time their personal information was shared with a third party. They were informed that they would receive an email report each time their data was shared with a third party containing a description of what data was shared and how and why the data were to be used. Those in the low cognitive control condition received no indication that they would know when their data was shared in the future.

After reading through the instructions pertaining to their specific experimental manipulation, the participants were asked a number of questions regarding their perceptions of control, privacy concerns, and attitudes toward the fictitious marketing organization sponsoring the research, as well as several measures used as manipulation checks to ensure the validity of the experimental procedure. After completing these measures, they were fully debriefed regarding the deceptive nature of the experiment and reassured that their browsing history had not been tracked and that their personal information would not be shared with any third-party organizations.

Analysis and Results

In this section, we detail the pre-analysis and data validation procedures undergone to establish construct validity and reliability of the measurement items used. After establishing these necessary pre-conditions, we proceed to evaluate the proposed model using SEM. All data validation and model testing was completed in R (R Core Team 2014) using the lavaan SEM package (Rosseel 2012).

Manipulation Checks and Sample Characteristics

It is necessary in experimental research to test whether the experimental manipulation(s) produced the intended effects. Manipulation checks were performed for the behavioral and cognitive control manipulations using measurement items gathered for this purpose. For behavioral control, the low behavioral control condition reported significantly lower perceived behavioral control (M = 2.72, SD = 1.44) than the high behavioral control group (M = 3.61, SD = 1.60), $t(90.1) = -2.80$, $p < .01$ (one-tailed). For cognitive control, the low cognitive control condition reported significantly lower cognitive control (M = 2.25, SD = 1.16) than the high cognitive control group (M = 2.76, SD = 1.46), $t(85.7) = -1.87$, $p < .05$ (one-tailed).

The initial pool of participants who completed the presurvey totaled 139. Just 108 of these participants responded when invited to complete the second portion of the study. A comparison of the initial and final participant groups did not reveal any significant differences in terms of demographic variables, privacy-related measures, or other factors. After filtering out incomplete responses and several participants who either missed attention-checking questions or were clearly not providing legitimate responses, the final sample consisted of 94 usable responses. This sample was 51% male, 65% Caucasian, and a large majority (85%) reported English as their primary language. They were young adults ($M_{age} = 21.2$, $SD = 1.76$) in their first few years of college ($M_{Yrs\ College} = 2.38$, $SD = 1.34$).

Establishing Construct Validity and Reliability

A first step in the pre-analysis was to establish factorial validity and the reliability of the measures used. Since most constructs and several relationships hypothesized in the model are derived from prior literature, we chose to use CFA to validate the measurement model. CFA is appropriate in situations where strong theory suggests known relationships among the indicators and their intended factors (Brown 2006), as in our case. Upon fitting the proposed measurement structure of the model, measurement items that loaded poorly onto their respective factors and reduced reliability were dropped. The refined model exhibited acceptable fit to the data ($\chi^2 = 105.17$, $df_{model} = 93$, $p = 0.183$, $\chi^2/df = 1.13$, CFI = 0.98, TLI = 0.98, RMSEA = 0.037, SRMR = 0.062). Satisfied that the model was a good fit to the data, we could then calculate correlations, reliabilities, and AVEs to further aid in establishing factorial validity. These metrics are summarized in Table 1.

Table 1. Construct Correlations, Reliabilities, and AVEs

Construct	CR	AVE	(1)	(2)	(3)	(4)	(5)
1. Attitudes toward organization	.772	.628	.792				
2. Perceived control	.867	.632	.284**	.795			
3. Privacy concerns	.916	.682	−.374***	−.439***	.826		
4. Disposition to trust	.802	.573	.028	.207*	−.160	.757	
5. Disposition to value privacy	.826	.621	−.133	−.146	.460***	.138	.788

Notes. N = 94; CR = Composite Reliability; AVE = average variance extracted; values along the diagonal are the square root of the AVE.
* = $p < 0.05$, ** = $p < 0.01$, *** = $p < 0.001$.

In order to demonstrate factorial validity, the AVE for a construct should be > 0.5 (convergent validity) (Hair et al. 2010). In addition, discriminant validity is demonstrated when the square root of a construct's AVE is higher than the correlation between that construct and all other constructs in the model (Hair et al. 2010). As shown in Table 1, the constructs in the model meet all of these criteria. To establish reliability, the composite reliability value should be > 0.7 (Fornell and Larcker 1981; Kock 2010; Nunnally and Bernstein 1994). The computed reliability values shown in Table 1 indicate sufficient reliabilities.

Evaluating Common-Methods Bias

Because all survey items were measured using the same method (an online survey), the possibility exists that some of the shared variance among the constructs is due to the common method rather than the underlying relationships among the constructs. Though precautions were implemented to reduce this likelihood (e.g., randomizing the order of survey items) (Straub et al. 2004), it is necessary to test for common-methods bias

in the measurement model. We first note that no correlations shown in Table 1 are above 0.90. Correlations above this threshold may indicate a common-methods bias (Pavlou et al. 2007). A second approach is called Harman's single factor test (Podsakoff et al. 2003), in which all measurement items are included in an exploratory factor analysis to see whether a single factor (the common method used) can explain a majority of the observed variance in the measures. While this method does not statistically control for method effects, it can be used as an effective diagnostic tool to identify whether common methods are negatively affecting results. Following the single factor test procedure, we included all items in an exploratory factor analysis and examined the (unrotated) solution. The single factor explained a mere 20% of the variance in the items, indicating that common methods bias was not negatively affecting the results of our analysis.

Having established the validity and reliability of the constructs measured, we now proceed to describe the SEM analysis of the full model.

Model Testing Results

We tested the theoretical model shown in Figure 1 using covariance-based SEM. We also included sex (female = 1), age, education, prior privacy invasion experiences, and privacy awareness as control variables for the endogenous constructs in the model. Only significant paths from the control variables were retained in the final model, as such removal did not significantly alter the other estimates in the model. The final model is shown in Figure 2 with model testing results. Fitting the structural model to the data produced generally acceptable indications of fit ($\chi^2 = 164.18$, $df_{model} = 139$, $p = 0.071$, $\chi^2/df = 1.18$, CFI = 0.97, TLI = 0.96, RMSEA = 0.043, SRMR = 0.072) (Hair et al. 2010). Hypothesized relationships shown in the theoretical model in Figure 1 were tested in conjunction with the SEM analysis. The tested hypotheses, along with their corresponding path estimates and significance levels, are summarized in Table 2. The testing results indicate general support for many of the relationships proposed in the model. These results are discussed in the context of their broader implications in the section that follows.

Table 2. Hypothesis Testing Results

Hypothesis	β	Support?
H1a. Disposition to trust → Perceived control	$.312^{**}$	**Yes**
H1b. Disposition to trust → (-) Privacy concerns	*n.s.*	No
H2a. Disposition to value privacy → (-) Perceived control	*n.s.*	No
H2b. Disposition to value privacy → Privacy concerns	$.391^{***}$	**Yes**
H3. Behavioral control → Perceived control	$.246^{*}$	**Yes**
H4. Cognitive control → Perceived control	*n.s.*	No
H5. Perceived control → (-) Privacy concerns	$-.404^{***}$	**Yes**
H6. Perceived control → Attitudes toward organization	$-.270^{*}$	**Yes**
H7. Privacy concerns → (-) Attitudes toward organization	$-.384^{**}$	**Yes**

Notes. * = $p < 0.05$, ** = $p < 0.01$, *** = $p < 0.001$.

Discussion

Many modern organizations collect large amounts of data from and about their customers (Vaidhyanathan 2011). These data are proving highly valuable (McKinsey Global Institute 2011), but such widespread collection of personal and behavioral information has been met with significant trepidation by the general public (Burst Media 2009; UK Information Commissioner's Office 2013), especially as this data collection has become nearly ubiquitous and difficult to fully prevent (Vertesi 2014). As more customers find out just how much data has been involuntarily collected about them, companies must balance the business value of large customer datasets against ethical considerations and the potential negative public opinion that results from breaches of privacy (George et al. 2014). Given these pressing managerial issues, this research develops and empirically tests a theoretical model that investigates the link between customer attitudes toward an organization and their perceptions of privacy issues when personal data has already been involuntarily collected. We draw on psychological stress literature to explore methods of returning a sense of control to individuals. We then model the downstream effects of this perceived control in the formation of privacy concerns, and we argue that these perceptions of control and IPC can have important effects on overall evaluations of

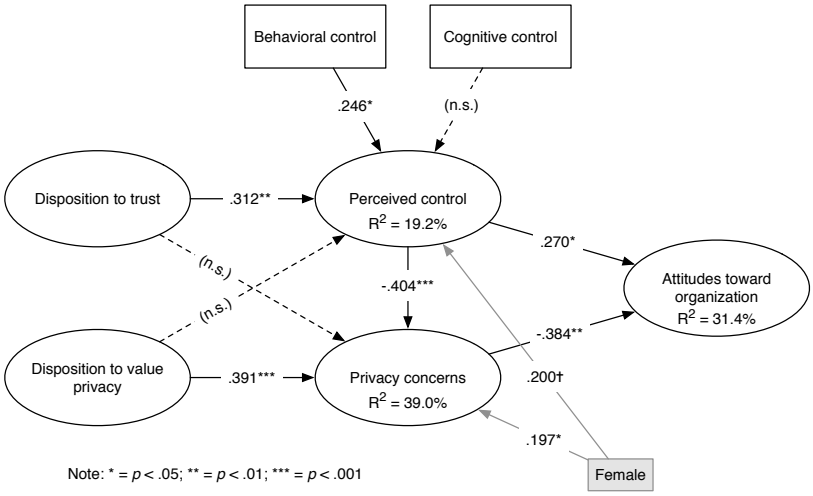

Figure 2. Final Research Model with Hypothesis Testing Results

the data-collecting organization. Our empirical model was tested using 94 experimental subjects, and most of the proposed relationships within the model received clear support. This section discusses the implications of these results, both in terms of theoretical development and the potential practical application of the concepts discussed.

We will now address the unsupported hypotheses regarding the effects of cognitive control and disposition to value privacy on perceived control. First, our empirical test showed no significant influence of cognitive control on perceived control, even though the psychological stress literature has clearly validated this construct as an effective means of increasing control and reducing anxiety in many different contexts. One plausible explanation for this (aside from the obviously small sample size) is that the effect of cognitive control may have been partially obviated by participants' baseline level of concern in the experiment. If some individuals' baseline level of concern in the scenario was low as a result of them not thinking in detail about the level of their personal exposure (a likely possibility with student subjects in an experiment), then the cognitive control manipulation may have pushed awareness beyond that baseline, which could actually amplify privacy concerns and reduce perceived control. This would have made the effect more ambiguous, and serves as a plausible explanation for the nonsignificant relationship indicated by the model testing results. Future research should more specifically examine the effects of cognitive control while accounting for a broader range of other possible effects in order to isolate the effect of that construct. The cognitive control construct has been clearly validated in other domains, and it may simply be that more methodological refinement is needed to obtain the intended effect within an experimental scenario.

Second, our analysis revealed a lack of statistical support for the influence of disposition to value privacy on perceived control. This hypothesis was derived based on the tendency for an individual who values privacy to feel less in control of the situation when a privacy violation occurs. It is possible that the relationship between these constructs was not supported due to the constraints of conducting laboratory research. In this research, participants were aware that they were engaged in a research study and thus may have felt that the invasion of privacy that occurred was fabricated and of marginal risk. Accordingly, participants may have maintained a perception of control over the situation rather than the hypothesized emotional state associated with a lack of control. Future research investigating perceptions of control should strive to incorporate as much realism as possible in the experimental design. Doing so will yield the most ecologically valid and generalizable results.

Finally, disposition to trust did not significantly influence privacy concerns. It is possible that the nature of our sample—young college students—negatively impacted our results. Young technology users have been engaging with various forms of technology for a majority of their lives. It is possible that technology users with such extensive experience maintain a general trusting demeanor whilst identifying privacy concerns

associated with *specific* technologies, organizations, or users that they have encountered over time. In other words, a general disposition to trust may not ensure a broad sentiment of reduced privacy concerns. This possibility represents an interesting avenue for future investigation.

Implications for Research

This research has important implications for privacy theory. Drawing from prior work in related contexts, the theory presented here is the first to examine IPC mitigation in an involuntary-disclosure context. Accordingly, we contribute theory to a disclosure domain in which very little understanding has yet been obtained, despite unprecedented amounts of involuntary disclosure occurring in online settings. The privacy models in other contexts may not translate well to an involuntary disclosure setting, since privacy has been identified as being highly context-dependent (Pavlou 2011; Smith et al. 2011). When disclosure has already occurred, the options available for organizations to manage users' IPC are limited compared to other contexts wherein a company offers various privacy assurances in order to convince the customer to disclose information. Given the widespread practice of involuntary data collection, and the increasing futility of avoiding such disclosure (Vertesi 2014), it is important for the IS community to offer effective theoretical guidance for companies grappling with these issues.

Two such solutions are presented in our theoretical model in the form of behavioral and cognitive control. We show that empowering users with behavioral control—by something as simple as enabling the user to verify the accuracy of their information and choose which third-party organizations their data will be shared with—can significantly increase those users' perceived control of their personal information. This control, in turn, mitigates IPC. These findings can be leveraged by future theorists as we continue to seek effective methods of increasing control and reducing privacy concerns, particularly in situations where options for offering privacy assurances are limited. In addition, we argue theoretically for the effect of cognitive control in producing an increased sense of control, building on substantial validation of this relationship in other domains. While our empirical test of this relationship did not indicate a significant influence on perceived control, there is still potential value for future research to build on these principles and further test other operationalizations of cognitive control in other scenarios. Taken together, these two constructs, which are drawn from the robust psychological stress literature (Averill 1973), constitute a fresh approach to exploring issues of control in the context of information privacy.

Finally, there are important implications for the influence of perceived control and IPC on participants' attitudinal assessments of the organization collecting the personal information. Prior research has linked IPC with more specific attitudes directed at a particular practice or activity, such as information collecting (Smith et al. 1996), secondary use (Culnan 1993), personalization (Chellappa and Sin 2005), and so on. With modern companies facing severe public scrutiny for their privacy-threatening activities (Best 2014; Herold 2014), it is crucial for IS researchers to examine whether privacy policy can directly affect how companies are viewed by their customers and potential customers. This research is directed squarely at the link between privacy-related perceptions and affective judgments of a company, and we show that increasing perceived control can indeed positively impact users' evaluations of the company. This effect is largely mediated through the mitigating effect of perceived control on IPC, which was even more strongly linked with attitudes toward the organization in our sample. There remain unanswered questions, however, regarding the full extent of the relationship between IPC and customer attitudes. For example, do individuals uniformly relate privacy practices with positive judgments of a company, or are there other moderating factors that would qualify this relationship? How does the effect of customers' IPC on their attitudes toward a company change over time? Is it possible for an organization to overcome a past grievance and repair their public image? These and other questions may lead to important theoretical insights, and the theory developed in this work can be leveraged in future work that tackles these issues.

Implications for Practice

Given the widespread collection and use of personal information, and the associated privacy issues inherent in this practice, this research has important practical contributions as well. Most importantly, online companies and other organizations involved in some form of involuntary data collection can, with relative ease,

implement the behavioral and cognitive control constructs proposed in the model. The manipulations in the experimental design constitute just a few of many potential methods to empower users with perceived control over the data being collected. Practitioners could apply the concepts of behavioral and cognitive control to aid in effectively managing privacy concerns by increasing users' sense of control over their online data.

The practical implications of the theory developed here are not limited to online companies, however. Many governmental organizations (e.g., the Transportation and Security Administration in the United States) are required to gather and evaluate highly sensitive information (e.g., full-body scans in many airports), and are constantly grappling with public opinion regarding the privacy implications of such mandatory disclosures (Ahlers 2013). These organizations gather private information in the interest of national security, and some such disclosure is acceptable to most citizens. Additional mechanisms that would allow these organizations to collect necessary information while managing privacy concerns could prove a valuable strategy. There are several potential practical applications of behavioral control that such an agency could employ. For example, it may be feasible to allow citizens access to verify that their information was recorded correctly. Another strategy would be to allow individuals to choose between a set of equally effective screening technologies, perhaps even with something as simple as choosing the color of ink used when taking fingerprints. All of these would allow individuals to feel that they were "in charge" of a portion of the privacy-threatening experience.

Likewise, we argue theoretically for the efficacy of cognitive control in providing individuals increased control, and this concept is also an excellent candidate for real-world application by government organizations. The main way in which cognitive control could be granted would be various forms of transparency regarding what data is being used, how and why it is being used, and so on. Particularly attractive is the fact that such transparency does not change the amount of data being collected or used, but rather provides individuals an explanation as to why. An interesting possibility would be an online portal through which an individual could easily see which organizations accessed a given piece of information and for what purpose. These and other methods could be used by any organizations that have certain data collection procedures that are effectively mandatory. Such organizations can use the concepts highlighted in this work to more effectively manage individual privacy concerns.

Further, as these companies and government organizations find effective ways of reducing privacy concerns, our findings indicate that this will have a direct impact on public opinion regarding the organization. Most modern organizations are keenly aware of the need to manage public opinion regarding privacy, and focus on gathering data that produce value while respecting their customers. Our findings indicate that giving users control over information collection will have a direct, positive impact on their evaluations of the organization. Enabling users with control also reduces IPC, which can have a profound impact on attitudes about the company, according to our findings. These recommendations constitute practical knowledge that can be applied by many different organizations to their benefit. In an environment where massive data collection is the norm, organizations will continually need effective ways to engage with the public regarding privacy issues.

Limitations and Future Research

As with any research study, our work has limitations that should be considered when interpreting our results and stated implications. By design, experiments sacrifice realism in favor of experimental control. We took measures to align the experimental privacy invasion with its real-world counterpart, but the participants knew they were participating in a study and may have been freer with their personal information or biased in their privacy-related evaluations than if their privacy had been violated in their everyday lives. Relatedly, our use of relatively young student subjects to study privacy issues may bias our results, given that younger individuals tend to evaluate privacy differently than the general population. While student subject pools tend to be more homogeneous and conducive to experimental research, we acknowledge the lack of generalizability as a limitation. These purposeful methodological choices were made to carefully examine the effects of behavioral and cognitive control, but there remains an opportunity for future research to evaluate these phenomena using field studies, which would grant greater generalizability to the theory.

Conclusion

Many modern organizations must carefully balance the practice of gathering large amounts of valuable data from individuals with the associated ethical considerations and potential negative public image inherent in breaches of privacy. As it becomes commonplace for many types of information to be collected without individuals' knowledge or consent, managers and researchers alike can benefit from understanding how individuals react to such involuntary disclosures, and how these reactions can impact evaluations of the data-collecting organizations. We have proposed and empirically tested a theoretical model to show how empowering individuals with a feeling of control over their personal information can help mitigate IPC following an invasion of privacy. We draw from the psychological stress literature to establish behavioral and cognitive control as effective mechanisms to increase perceived control, and show that increasing control and reducing IPC can significantly influence individuals' attitudes toward the organization that has committed the privacy invasion. Our theory provides an initial look at managing privacy concerns in an involuntary disclosure context that future research can build on. Furthermore, modern organizations can use the mechanisms identified in our model to build effective strategies for engaging with the public regarding the collection and protection of private information.

References

Adams, B. 2012. "2012: The Year the World Fell Out of Love with Google," (available online at http://www.stateofdigital.com/2012-the-year-the-world-fell-out-of-love-with-google; accessed Feb. 18, 2015).

Ahlers, M. M. 2013. "TSA Removes Body Scanners Criticized as Too Revealing," (available online at http://www.cnn.com/2013/05/29/travel/tsa-backscatter/; accessed Feb. 18, 2015).

Alge, B. J. 2001. "Effects of Computer Surveillance on Perceptions of Privacy and Procedural Justice," *Journal of Applied Psychology* (86:4), pp. 797–804.

Altman, I. 1975. *The Environment and Social Behavior: Privacy, Personal Space, Territory, and Crowding,* Monterey, CA: Brooks/Cole Publishing.

Angst, C. M. and Agarwal, R. 2009. "Adoption of Electronic Health Records in the Presence of Privacy Concerns: The Elaboration Likelihood Model and Individual Persuasion," *MIS Quarterly* (33:2), pp. 339–370.

Arcand, M., Nantel, J., Arles Dufour, M., and Vincent, A. 2007. "The Impact of Reading a Web Site's Privacy Statement on Perceived Control over Privacy and Perceived Trust," *Online Information Review* (31:5), pp. 661–681.

Averill, J. R. 1973. "Personal Control over Aversive Stimuli and its Relationship to stress," *Psychological Bulletin* (80:4), pp. 286–303.

Bandura, A. 1991. "Social Cognitive Theory of Self-regulation," *Organizational Behavior and Human Decision Processes* (50:2), pp. 248–287.

Bansal, G., Zahedi, F., and Gefen, D. 2010. "The Impact of Personal Dispositions on Information Sensitivity, Privacy Concern and Trust in Disclosing Health Information Online," *Decision Support Systems* (49:2), pp. 138–150.

Bélanger, F., Hiller, J. S., and Smith, W. J. 2002. "Trustworthiness in Electronic Commerce: The Role of Privacy, Security, and Site Attributes," *Journal of Strategic Information Systems* (11:3-4), pp. 245–270.

Best, J. 2014. "Google, Facebook, Twitter Face Lawsuit over 'Illegible, Incomprehensible' Privacy Policies," (available online at http://www.zdnet.com/google-facebook-twitter-face-lawsuit-over-illegible-incomprehensible-privacy-policies-7000027780/; accessed Feb. 18, 2015).

Brown, T. A. 2006. *Confirmatory Factor Analysis for Applied research,* New York: Guilford Press.

Brown, T. J. and Dacin, P. A. 1997. "The Company and the Product: Corporate Associations and Consumer Product Responses," *Journal of Marketing* (61:1), pp. 68–84.

Burkert, H. 1997. "Privacy-enhancing Technologies: Typology, Critique, Vision," in *Technology and privacy,* MIT Press, pp. 125–142.

Burst Media 2009. "Online Privacy Still A Consumer Concern," (available online at http://www.burstmedia.com/pdf/2009_02_01.pdf; accessed Feb. 18, 2015).

Carlsson, K., Andersson, J., Petrovic, P., Petersson, K. M., Öhman, A., and Ingvar, M. 2006. "Predictability Modulates the Affective and Sensory-discriminative Neural Processing of Pain," *Neuroimage* (32:4), pp. 1804–1814.

Chellappa, R. K. and Sin, R. G. 2005. "Personalization Versus Privacy: An Empirical Examination of the Online Consumer's Dilemma," *Information Technology & Management* (6:2-3), pp. 181–202.

Chen, K. and Rea Jr, A. L. 2004. "Protecting Personal Information Online: A Survey of User Privacy Concerns and Control Techniques," *Journal of Computer Information Systems* (44:4), pp. 85–92.

Colquitt, J. A., Scott, B. A., and LePine, J. A. 2007. "Trust, Trustworthiness, and Trust Propensity: A Meta-analytic Test of Their Unique Relationships with Risk Taking and Job Performance," *Journal of Applied Psychology* (92:4), pp. 909–927.

Cranor, L. F., Guduru, P., and Arjula, M. 2006. "User Interfaces for Privacy Agents," *ACM Transactions on Computer-Human Interaction* (13:2), pp. 135–178.

Culnan, M. J. 1993. ""How Did They Get My Name?": An Exploratory Investigation of Consumer Attitudes toward Secondary Information Use," *MIS Quarterly* (17:3), pp. 341–363.

Culnan, M. J. and Armstrong, P. K. 1999. "Information Privacy Concerns, Procedural Fairness, and Impersonal Trust: An Empirical Investigation," *Organization Science* (10:1), pp. 104–115.

Culnan, M. J. and Bies, R. J. 2003. "Consumer Privacy: Balancing Economic and Justice Considerations," *Journal of Social Issues* (59:2), pp. 323–342.

Dennis, A. R. and Valacich, J. S. 2001. "Conducting Experimental Research in Information Systems," *Communications of the AIS* (7).

Dinev, T., Bellotto, M., Hart, P., Russo, V., Serra, I., and Colautti, C. 2006. "Privacy Calculus Model in e-Commerce: A Study of Italy and the United States," *European Journal of Information Systems* (15:4), pp. 389–402.

Dinev, T. and Hart, P. 2004. "Internet Privacy Concerns and Their Antecedents: Measurement Validity and a Regression Model," *Behaviour & Information Technology* (23:6), pp. 413–423.

Dinev, T. and Hart, P. 2006. "An Extended Privacy Calculus Model for e-Commerce Transactions," *Information Systems Research* (17:1), pp. 61–80.

Dinev, T., Hart, P., and Mullen, M. R. 2008. "Internet Privacy Concerns and Beliefs about Government Surveillance: An Empirical Investigation," *The Journal of Strategic Information Systems* (17:3), pp. 214–233.

Dzewaltowski, D. A., Noble, J. M., and Shaw, J. M. 1990. "Physical Activity Participation: Social Cognitive Theory Versus the Theories of Reasoned Action and Planned Behavior," *Journal of Sport & Exercise Psychology* (12:4), pp. 388–405.

Endler, N. S., Speer, R. L., Johnson, J. M., and Flett, G. L. 2001. "General Self-efficacy and Control in Relation to Anxiety and Cognitive Performance," *Current Psychology* (20:1), pp. 36–52.

Faranda, W. T. 2001. "A Scale to Measure the Cognitive Control Form of Perceived Control: Construction and Preliminary Assessment," *Psychology & Marketing* (18:12), pp. 1259–1281.

Fila, M. J., Paik, L. S., Griffeth, R. W., and Allen, D. 2014. "Disaggregating Job Satisfaction: Effects of Perceived Demands, Control, and Support," *Journal of Business and Psychology* (29:4), pp. 639–649.

Fornell, C. and Larcker, D. F. 1981. "Evaluating Structural Equation Models with Unobservable Variables and Measurement Error," *Journal of Marketing Research* (18:1), pp. 39–50.

Forrest, C. 2015. TechRepublic (ed.). 2015. (Available online at http://www.techrepublic.com/article/windows-10-violates-your-privacy-by-default-heres-how-you-can-protect-yourself/;).

Ganster, D. C. 1989. "Worker Control and Well-being: A Review of Research in the Workplace," *Job Control and Worker Health* (3:23), pp. 213–229.

George, G., Haas, M. R., and Pentland, A. 2014. "Big Data and Management," *Academy of Management Journal* (57:2), pp. 321–326.

Giles, M. 2010. "A World of Connections: A Special Report on Social Networking," (available online at http://www.economist.com/node/15351002; accessed Feb. 18, 2015).

Goodwin, C. 1991. "Privacy: Recognition of a Consumer Right," *Journal of Public Policy & Marketing* (10:1), pp. 149–166.

Hair, J., Black, W., Babin, B., and Anderson, R. 2010. *Multivariate Data Analysis,* Englewood Cliffs, NJ: Prentice-Hall.

Herold, B. 2014. "Google Under Fire for Data-Mining Student Email Messages," *Education Week* (33), pp. 22–23.
Hoadley, C. M., Xu, H., Lee, J. J., and Rosson, M. B. 2009. "Privacy as Information Access and Illusory Control: The Case of the Facebook News Feed Privacy Outcry," *Electronic Commerce Research and Applications* (9:1), pp. 1–11.
Hockey, G. R. J. and Earle, F. 2006. "Control Over the Scheduling of Simulated Office Work Reduces the Impact of Workload on Mental Fatigue and Task Performance," *Journal of Experimental Psychology: Applied* (12:1), pp. 50–65.
Hong, W. and Thong, J. 2013. "Internet Privacy Concerns: An Integrated Conceptualization and Four Empirical Studies," *MIS Quarterly* (37:1), pp. 275–298.
Jarvenpaa, S. L., Knoll, K., and Leidner, D. E. 1998. "Is Anybody Out There? Antecedents of Trust in Global Virtual Teams," *Journal of Management Information Systems* (14:4), pp. 29–64.
Johnson, B. 2010. "Privacy No Longer a Social Norm, says Facebook Founder," (available online at http://www.theguardian.com/technology/2010/jan/11/facebook-privacy; accessed Feb. 18, 2015).
Jones, S. 2009. "Generations Online in 2009," (available online at http://www.pewinternet.org/files/old-media/Files/Reports/2009/PIP_Generations_2009.pdf; accessed Feb. 18, 2015).
Keith, M. J., Thompson, S. C., Hale, J., Lowry, P. B., and Greer, C. 2013. "Information Disclosure on Mobile Devices: Re-examining Privacy Calculus with Actual User Behavior," *International Journal of Human-Computer Studies* (71:12), pp. 1163–1173.
Kock, N. 2010. *WarpPLS 1.0 User Manual*. Tech. rep. Laredo, Texas, USA.
Langer, E. J., Janis, I. L., and Wolfer, J. A. 1975. "Reduction of Psychological Stress in Surgical Patients," *Journal of Experimental Social Psychology* (11:2), pp. 155–165.
Laufer, R. S. and Wolfe, M. 1977. "Privacy as a Concept and a Social Issue: A Multidimensional Developmental Theory," *Journal of social Issues* (33:3), pp. 22–42.
Li, H., Sarathy, R., and Xu, H. 2010. "Understanding Situational Online Information Disclosure as a Privacy Calculus," *The Journal of Computer Information Systems* (51:1), pp. 62–71.
Li, Y. 2011. "Empirical Studies on Online Information Privacy Concerns: Literature Review and an Integrative Framework," *Communications of the AIS* (28), pp. 453–496.
Li, Y. 2014a. "A Multi-level Model of Individual Information Privacy Beliefs," *Electronic Commerce Research and Applications* (13:1), pp. 32–44.
Li, Y. 2014b. "The Impact of Disposition to Privacy, Website Reputation and Website Familiarity on Information Privacy Concerns," *Decision Support Systems* (57), pp. 343–354.
Lu, Y., Tan, B., and Hui, K.-L. 2004. "Inducing Customers to Disclose Personal Information to Internet Businesses with Social Adjustment Benefits," in *Proceedings of the 25th International Conference on Information Systems,* Washington, DC, pp. 272–281.
Malhotra, N. K., Kim, S. S., and Agarwal, J. 2004. "Internet Users' Information Privacy Concerns (IUIPC): The Construct, the Scale, and a Causal Model," *Information Systems Research* (15:4), pp. 336–355.
Margulis, S. T. 2003a. "On the Status and Contribution of Westin's and Altman's Theories of Privacy," *Journal of Social Issues* (59:2), pp. 411–429.
Margulis, S. T. 2003b. "Privacy as a Social Issue and Behavioral Concept," *Journal of Social Issues* (59:2), pp. 243–261.
Martin, D., Wu, H., and Alsaid, A. 2003. "Hidden Surveillance by Web sites: Web Bugs in Contemporary Use," *Communications of the ACM* (46:12), pp. 258–264.
Mayer, R. C., Davis, J. H., and Schoorman, F. D. 1995. "An Integrative Model of Organizational Trust," *Academy of Management Review* (20:3), pp. 709–734.
McKinsey Global Institute 2011. "Big Data: The Next Frontier for Innovation, Competition, and Productivity," (available online at http://www.mckinsey.com/insights/business_technology/big_data_the_next_frontier_for_innovation; accessed Feb. 18, 2015).
McKnight, D. H., Cummings, L. L., and Chervany, N. L. 1998. "Initial Trust Formation in New Organizational Relationships," *Academy of Management Review* (23:3), pp. 473–490.
Metzger, M. J. 2004. "Privacy, Trust, and Disclosure: Exploring Barriers to Electronic Commerce," *Journal of Computer-Mediated Communication* (9:4).

Milne, G. R. and Rohm, A. J. 2000. "Consumer Privacy and Name Removal across Direct Marketing Channels: Exploring Opt-in and Opt-out Alternatives," *Journal of Public Policy & Marketing* (19:2), pp. 238–249.
Milne, G. R., Rohm, A. J., and Bahl, S. 2004. "Consumers' Protection of Online Privacy and Identity," *Journal of Consumer Affairs* (38:2), pp. 217–232.
Miyazaki, A. D. 2012. "Online Privacy and the Disclosure of Cookie Use: Effects on Consumer Trust and Anticipated Patronage," *Journal of Public Policy & Marketing* (27:1), pp. 19–33.
Morton, A. "Measuring Inherent Privacy Concern and Desire for Privacy: A Pilot Survey Study of an Instrument to Measure Dispositional Privacy Concern," in *2013 International Conference on Social Computing (SocialCom),* IEEE, pp. 468–477.
Müller, M. J. 2011. "Will It Hurt Less If I Believe I Can Control It? Influence of Actual and Perceived Control on Perceived Pain Intensity in Healthy Male Individuals: A Randomized Controlled Study," *Journal of Behavioral Medicine* (35:5), pp. 529–537.
Namasivayam, K. 2004. "Action Control, Proxy Control, and Consumers' Evaluations of the Service Exchange," *Psychology & Marketing* (21:6), pp. 463–480.
Norberg, P. A. 2007. "The Privacy Paradox: Personal Information Disclosure Intentions Versus Behaviors," *Journal of Consumer Affairs* (41:1), pp. 100–126.
Nunnally, J. C. and Bernstein, I. H. 1994. *Psychometric Theory,* New York: McGraw-Hill.
Patil, S. and Kobsa, A. 2005. *Uncovering Privacy Attitudes and Practices in Instant Messaging,* New York: ACM.
Pavlou, P. A. 2011. "State of the Information Privacy Literature: Where Are We Now and Where Should We Go?," *MIS Quarterly* (35:4), pp. 977–988.
Pavlou, P. A., Liang, H., and Xue, Y. 2007. "Understanding and Mitigating Uncertainty in Online Exchange Relationships: A Principal-agent Perspective," *MIS Quarterly* (31:1), pp. 105–136.
Phelps, J. E., D'Souza, G., and Nowak, G. J. 2001. "Antecedents and Consequences of Consumer Privacy Concerns: An Empirical Investigation," *Journal of Interactive Marketing* (15:4), pp. 2–17.
Podsakoff, P. M., MacKenzie, S. B., Lee, J. Y., and Podsakoff, N. P. 2003. "Common Method Biases in Behavioral Research: A Critical Review of the Literature and Recommended Remedies," *Journal of Applied Psychology* (88:5), pp. 879–903.
R Core Team 2014. *R: A Language and Environment for Statistical Computing*. R Foundation for Statistical Computing.
Rensel, A. D., Abbas, J. M., and Rao, H. R. 2006. "Private Transactions in Public Places: An Exploration of the Impact of the Computer Environment on Public Transactional Web Site Use," *Journal of the Association for Information Systems* (7:1), pp. 19–51.
Richards, R. J. 2012. "A Study of the Intent to Fully Utilize Electronic Personal Health Records in the Context of Privacy and Trust," PhD thesis, pp. 1–231.
Rosseel, Y. 2012. "lavaan: An R Package for Structural Equation Modeling," *Journal of Statistical Software* (48:2), pp. 1–36.
Rotter, J. B. 1971. "Generalized Expectancies for Interpersonal Trust," *American Psychologist* (26:5), pp. 443–452.
Salomons, T. V., Johnstone, T., Backonja, M.-M., and Davidson, R. J. 2004. "Perceived Controllability Modulates the Neural Response to Pain," *The Journal of Neuroscience* (24:32), pp. 7199–7203.
Sheehan, K. B. 1999. "An Investigation of Gender Differences in On-line Privacy Concerns and Resultant Behaviors," *Journal of Interactive Marketing* (13:4), pp. 24–38.
Sheehan, K. B. 2005. "In Poor Health: An Assessment of Privacy Policies at Direct-to-consumer Web Sites," *Journal of Public Policy & Marketing* (24:2), pp. 273–283.
Sheehan, K. B. and Hoy, M. G. 2000. "Dimensions of Privacy Concern among Online Consumers," *Journal of Public Policy & Marketing* (19:1), pp. 62–73.
Skinner, E. A. 1996. "A Guide to Constructs of Control," *Journal of Personality and Social Psychology* (71:3), pp. 549–570.
Smith, H. J., Dinev, T., and Xu, H. 2011. "Information Privacy Research: An Interdisciplinary Review," *MIS Quarterly* (35:4), pp. 989–1016.
Smith, H. J., Milberg, S. J., and Burke, S. J. 1996. "Information Privacy: Measuring Individuals' Concerns about Organizational Practices," *MIS Quarterly* (20:2), pp. 167–196.

Solove, D. J. 2002. "Conceptualizing Privacy," *California Law Review* (90:4), pp. 1087–1155.
Son, J. Y. and Kim, S. S. 2008. "Internet Users' Information Privacy-protective Responses: A Taxonomy and a Nomological Model," *MIS Quarterly* (32:3), pp. 503–529.
Staub, E., Tursky, B., and Schwartz, G. E. 1971. "Self-control and Predictability: Their Effects on Reactions to Aversive Stimulation," *Journal of Personality and Social Psychology* (18:2), pp. 157–162.
Straub, D., Boudreau, M.-C., and Gefen, D. 2004. "Validation Guidelines for IS Positivist Research," *Communications of the AIS* (13), pp. 380–427.
Tate, R. 2009. "Google CEO: Secrets Are for Filthy People," (available online at http://gawker.com/5419271/google-ceo-secrets-are-for-filthy-people; accessed Feb. 18, 2015).
Tsai, J., Egelman, S., Cranor, L., and Acquisti, A. 2011. "The Effect of Online Privacy Information on Purchasing Behavior: An Experimental Study," *Information Systems Research* (22:2), pp. 254–268.
Tucker, C. E. 2014. "Social Networks, Personalized Advertising, and Privacy Controls," *Journal of Marketing Research* (51:5), pp. 546–562.
UK Information Commissioner's Office 2013. "Annual Track 2013: Individuals," (available online at https://ico.org.uk/media/about-the-ico/documents/1042195/annual-track-2012-individuals.pdf; accessed Feb. 18, 2015).
Vaidhyanathan, S. 2011. "Welcome to the Surveillance Society," *IEEE Spectrum* (48:6), pp. 48–51.
Vertesi, J. 2014. "TMI: Theorizing Big Data," in *Theorizing the Web,* Brooklyn, NY.
Walczuch, R. and Lundgren, H. 2004. "Psychological Antecedents of Institution-based Consumer Trust in e-Retailing," *Information & Management* (42:1), pp. 159–177.
Westin, A. F. 1967. *Privacy and Freedom,* New York: Atheneum.
Xu, H. 2007. "The Effects of Self-Construal and Perceived Control on Privacy Concerns," in *ICIS 2007 Proceedings,* Citeseer, pp. 1–14.
Xu, H., Dinev, T., Smith, H. J., and Hart, P. 2008. "Examining the Formation of Individual's Privacy Concerns: Toward an Integrative View," in *ICIS 2008 Proceedings,* pp. 1–17.
Xu, H., Dinev, T., Smith, H. J., and Hart, P. 2011. "Information Privacy Concerns: Linking Individual Perceptions with Institutional Privacy Assurances," *Journal of the Association for Information Systems* (12:12), pp. 798–824.
Xu, H. and Teo, H.-H. 2004. "Alleviating Consumers' Privacy Concerns in Location-Based Services: A Psychological Control Perspective," in *ICIS 2004 Proceedings,* pp. 793–806.
Xu, H., Teo, H.-H., Tan, B. C. Y., and 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), pp. 135–173.
Xu, H., Teo, H.-H., Tan, B. C. Y., and Agarwal, R. 2012. "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), pp. 1342–1363.
Yao, M. Z. and Zhang, J. 2008. "Predicting User Concerns about Online Privacy in Hong Kong," *CyberPsychology & Behavior* (11:6), pp. 779–781.