Behaviors, Adverse Events, and Dispositions: An Empirical Study of Online Discretion and Information Control

Coye Cheshire and Judd Antin
School of Information, University of California, Berkeley, 102 South Hall, Berkeley, CA 94720-4600.
E-mail: {coye, jantin}@ischool.berkeley.edu

Elizabeth Churchill
Yahoo! Research, 2821 Mission College Blvd., Santa Clara, CA 95054.
E-mail: echu@yahoo-inc.com

In this article, the authors develop hypotheses about three key correlates of attitudes about discretionary online behaviors and control over one's own online information: frequency of engaging in risky online behaviors, experience of an online adverse event, and the disposition to be more or less trusting and cautious of others. Through an analysis of survey results, they find that online adverse events do not necessarily relate to greater overall Web discretion, but they do significantly associate with users' perceptions of Web information control. However, the frequencies with which individuals engage in risky online activities and behaviors significantly associate with both online discretion and information control. In addition, general dispositions to trust and be cautious are strongly related to prudent Internet behavior and attitudes about managing personal online information. The results of this study have clear consequences for our understanding of behaviors and attitudes that might lead to greater online social intelligence, or the ability to make prudent decisions in the presence of Internet uncertainties and risks. Implications for theory and practice are discussed.

Introduction

Online interaction favors the brave because "In important ways, using the Internet involves a leap of faith" (Bargh & McKenna, 2004, p. 585). In the presence of uncertainty, a convenient response is to recognize what one does not know and categorically avoid risky online interactions and systems. Alternatively, one can charge forward into uncertain interactions, oblivious (or selectively inattentive) to prospective threats. However, the most venerable and rewarding long-term strategy may be to act with discretion based on learned experiences, including encounters with prior threats. If individuals wish to take advantage of potentially rewarding online environments, the price is arguably learning to recognize risks in the presence of uncertainty and adapt over time.

The earliest discussions of the Internet tended to fall on one of two extremes, finding "utopians and doomsayers at odds" (DiMaggio, Hargittai, Neuman, & Robinson, 2001, p. 319). Early studies of online interaction highlighted the limitless possibilities of large-scale interaction and communication where geography no longer defined community (Foster, 1996; Rheingold, 2000). The Internet was also presented as a great liberator, providing social inclusion for the physically, materially, and socially disadvantaged (Turkle, 1995). Most of this early research also showed cautious optimism, demonstrating that certain characteristics and social categories could be manipulated and controlled online, potentially freeing individuals of marginalization from stereotypes and discrimination (Burkhalter, 1999; O'Brien, 1999). In addition to interpersonal interactions, online financial exchanges were portrayed as a brave new world for commerce (Burke, 2002; Wolfinbarger & Gilly, 2001), although they ultimately failed to replace traditional retail shopping and financial transactions (Grewal, Iyer, & Levy, 2004).

At the opposite extreme, the Internet has been described as a virtual mine-field, rife with threats to security and privacy. The unregulated character of the Internet led some to highlight the dangers of sexually explicit material, hate speech, and personal indiscretion as ideological bogeymen that were invading the terra firma of cyberspace (e.g., Sardar, 1995). These dangers "can be found in the space dubbed by some on the moral right an 'electronic Sodom' " (Valentine & Holloway, 2001, p. 71). In addition to ethical concerns,

Received December 1, 2009; revised February 23, 2010; accepted March 7, 2010

 DOI: 10.1002/asi.21346

even basic forms of financial transactions and interpersonal interaction were described as potentially threatening. By the late 1990s, approximately 80% of Internet users and online consumers already indicated concern about online threats to privacy (Oberndorf, 1998). Researchers and commentators alike (e.g., Beatty, 1996; Caudill & Murphy, 2000) warned that our activities on the Web could be tracked and mined for the benefit of commercial, government, or other unknown, nefarious parties.

As with all complex social and technical systems, the Internet is poorly described by the views at the periphery. Online systems can provide incredible possibilities and contribute to interaction and close relationship formation under the protection of anonymity (Bargh & McKenna, 2004). However, online interactions also involve significant risks that are not always easy to recognize and control. How and when individuals perceive uncertainty and risk are arguably *the* central problems for understanding online behavior. We address these problems in this article by investigating the connection between behavioral, attitudinal, and dispositional factors with discretionary online behaviors and attitudes about control over one's own information. Drawing from current theory and research, we develop several hypotheses and conduct survey analyses to investigate three key correlates of attitudes about Web discretion and Web information control: (1) frequency of engaging in risky online behaviors, (2) experience of an online adverse event, and (3) the disposition to be more or less trusting and cautious of others.

Mitigating and Managing Online Risk: Web Discretion and Information Control

When individuals interact with Internet systems, they develop implicit or explicit attitudes about the risks and uncertainties in online environments. Over time, expectations develop about the reliability, credibility, and security of online information systems. Colloquially, the varying levels of risk and uncertainty inherent in these expectations are often described as a problem of trust. However, what we think of as *trust* in a human being is more appropriately described as *confidence* in the context of an information system (Cheshire & Cook, 2004; Nissenbaum, 2004). Unlike interpersonal trust, in which uncertainty and risk stems from the possibility of another individual's betrayal (McLeod, 2008), Web sites and information systems cannot betray because they lack the agency and consciousness to do so (Friedman, Kahn, & Howe, 2000). Online systems can, however, fail users' expectations (i.e., they can be unreliable); present false, misleading, or incomplete information (i.e. they can lack credibility); or fail to guard information and services from potentially malicious others (i.e., they can be insecure).

Designers, programmers, and practitioners are able to influence the actions and behaviors of the online systems they create and maintain. These individuals are ultimately accountable for malfeasance, fraud, or deceit that occurs in the context of the systems they manage or design (Fiore & Cheshire, 2010). In this view, the online system can be a surrogate for the decisions of its designers, and attitudes about trust can influence our confidence in systems (Friedman et al., 2000). As Bargh and McKenna (2004) argue, "to trust or not to trust our interaction partners or Web site operators is an important moderator of how we respond to the 'limited bandwidth' and relative lack of information over the Internet" (p. 585).

Some researchers contend that humans can trust information (Kelton, Fleischmann, & Wallace, 2008) based on research that demonstrates how individuals behave towards computers and information systems (e.g., Kiesler & Sproull, 1997). Indeed, users often self-report that they are distrustful of new information and communication technologies, especially when these technologies intersect with privacy issues (Cheung & Lee, 2006; Strickland & Hunt, 2004). For other researchers of risky online interactions such as e-commerce transactions, conceptualizing relational human-to-system trust is largely disregarded in favor of its antecedent: perceived *trustworthiness* of the Web site or service (Lee & Turban, 2001). Despite the intellectual differences in terminology, most agree that trust-like concepts such as trustworthiness, credibility, and security are regarded as primary facilitators of constructive experiences on the Internet. For these reasons, "trust" and its related concepts should be designed into online systems (Shneiderman, 2000).

A crucial similarity between the concepts of trust and confidence is a shared focus on risk and uncertainty (Friedman et al., 2000). *Risk* describes what is at stake in a given interaction, whereas *uncertainty* captures one's level of confidence about a given outcome (Cook, Yamagishi, et al., 2005). Just as individuals have different tolerances for uncertainty and risk in interpersonal interactions, they also have varying acceptance of risk and uncertainty when interacting with online systems. The willingness or reluctance to engage in risky or uncertain situations is a critical part of understanding human behavior. Those who shy away from risk and uncertainty may fail to take advantage of opportunities to interact, entertain, and profit from these experiences (cf. Yamagishi, 2001). On the Internet, individuals who evade risky and uncertain situations may choose to interact in extremely circumscribed online environments, rarely moving beyond trusted Internet services and sites.

We investigate two distinct, but related ways that individuals can mitigate and manage the risks that they encounter in uncertain online environments. The first approach includes intentionally limiting oneself to trusted Web sites and diligently reading online information to alleviate potential harms. These behaviors lessen exposure to Internet risks through vigilance, demonstrating experience rather than carelessness or unconditional Internet avoidance. The second method for managing online risk is taking control of one's own personal information on the Internet. We are interested in individuals' *belief* that they have the power and capacity to manage their own information, rather than the objective accuracy of their presumed ability. Together, discretionary behaviors and perceptions of information control provide an

DOI: 10.1002/asi

inclusive view of individual agency and awareness in risky and uncertain online environments.

A crucial aspect of our investigation of Internet behaviors, attitudes, and beliefs is the associational relationship between these concepts. Beliefs and behaviors in online or offline settings are intrinsically linked and often mutually reinforced by one another. One's belief about the dangers of Internet interactions can influence online behaviors. Similarly, behavioral choices and circumstances can affect beliefs and attitudes about online interaction. For these reasons, we acknowledge the reciprocal relationship between these concepts in our theoretical and methodological discussions that follow.

Web Discretion

We refer to individuals' tendencies to (1) proactively avoid risky or harmful online situations, and (2) judiciously read information on Web sites as indicators of *Web discretion*. Individuals who employ greater Web discretion are more selective, carefully evaluating information and adjusting behavior based on perceptions of risks and uncertainties on the Internet. Such individuals are vigilant and meticulous about assessing and responding to online threats and mendacious information. On the other hand, individuals with lower Web discretion are less likely to discriminate between content and activities that engender varying levels of risk and uncertainty. A lack of Web discretion denotes an inability or reluctance to respond to changing contexts and selectively protect oneself from harm or misinformation.

An important indicator of an individual's perception of online risk is the strategy she or he employs for dealing with potential threats. In a survey analysis, Fox (2000) found that a sizable percentage of respondents reported using tactics such as providing fake personal information to deal with online risks. More recent research by the Pew Research Center echoes this finding, noting that 46% of teens who have public online profiles intentionally provide false information for protection or as a form of play (Ranie & Tancer, 2007). Those who are less concerned about online dangers are unlikely to take actions to protect themselves. Thus, it is logical to assume that increasing levels of concern beget greater protective behaviors and precautions. However, this effect is not necessarily supported by empirical research. Individuals who perceive fairly high online risk still choose to participate in risky transactions (Corbitt, Thanasankit, & Yi, 2003). Even though a clear majority of Internet users report that they are concerned about privacy issues, research shows that very few people actually engage in behaviors to alleviate this anxiety (Perez, 2009).

Perhaps the most fundamental way to reduce online risk is to interact with Web sites that one already deems trustworthy. For example, trust in certain types of Web sites or e-commerce transactions correlates with lower perceptions of risk and uncertainty when purchasing products (Kim & Han, 2009). Different features of Web sites can encourage perceptions of trustworthiness, such as navigational structure (Vance, Elie-Dit-Cosaque, & Straub, 2008), ease of use (Gefen, Karahanna, & Straub, 2003), and use of other content and social cues (Fogg, 2003; Wang & Emurian, 2005). Beyond the behavioral and self-reported determinants of Web site trustworthiness and credibility, an equally important factor is whether an individual *believes* that he or she restricts herself to established, trustworthy Web sites. Furthermore, carefully reading online information from online sources, trusted or not, is an important means of protecting oneself from potential harm. Even cursory evaluations of Web site policy and privacy notices are used as strategies by individuals to manage the risks of disclosing personal information (Milne & Culnan, 2004).

Web Information Control

Concerns about how personal information will be handled on the Internet have grown alongside the explosive growth of voluntary information sharing and online personal disclosure. Attention to the dangers of online personal information has in part been driven by a variety of high-profile scams and other forms of malfeasance (e.g., Jones, 2008; Sterling, 2005). We refer to an individual's perception that she has control over her personal information on the Internet as *Web information control.* Control over one's own information is synonymous with information privacy control: "the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others" (Westin, 1967, p. 7). Although the definition itself is uncomplicated, the reality of information control and privacy is that these concepts are rarely consistent, widely varying by culture, industry, and regulatory laws (Malhotra, Kim, & Agarwal, 2004).

Control over one's own information is a key element of privacy in online financial transactions (Chen & Rea, 2004; Malhotra et al., 2004) and other forms of Internet interaction (Olivero & Lunt, 2004). Information technology changes so quickly on the Internet that individuals often violate their own privacy without realizing how their digital identifiers (e.g., e-mail addresses, usernames, uniform resource locators [URLs]) are stored and used by others (Gross, 2009). Phelps and his colleagues define privacy in terms of, "who has access to personal data (i.e., disclosure), how personal data are used (i.e., appropriation and false light), and what volume of advertising and marketing offers arise from the use of personal data" (Phelps, Nowak, & Ferrell, 2000, p. 29). In their multidimensional analysis of Internet users' information privacy concerns, Malholtra et al. (2004) demonstrate that the perception of control over one's information is one of three first-order factors of online privacy, along with beliefs about the equitable exchange of information and awareness of how personal information will be used by others. In addition, Olivero and Hunt (2004) use qualitative interviews to find similar evidence of widespread concerns about one's ability to control their own information and the complex Internet environments where personal information is collected.

DOI: 10.1002/asi

The dramatic rise in the popularity of social networking sites (SNSs) changed the scale of personal information made available on the Web. The number of American adults who use social networking sites such as MySpace, Facebook, or LinkedIn exploded from 8% in 2005 to 46% in 2009 (Lenhart, 2009). Systems such as Facebook create value for users by closely tracking individual behavior, and subsequently advertising this information to others. In exchange for free services, users share large amounts of potentially sensitive information. Amazingly, individuals offer this information willingly; even when the privacy and rules of ownership are in constant flux (see Sullivan, 2009; Walters, 2009a, 2009b). Although some online systems allow users to determine which information about them is tracked or shared, others do not. Furthermore, simply navigating to various Web sites leaves trails of information behind (Gross, 2009), sometimes despite protective measures available in popular Web browsers (Gomez, Pinnick, & Soltani, 2009).

The potential for user backlash and unintended consequences of personal information sharing has grown alongside technological advances in tracking (e.g., Read, 2006), forcing leading online systems such as Facebook to backpedal and provide users with greater control over their information (Wortham, 2009). When entirely new systems are released that appear to violate norms of personal disclosure, the furor over privacy can largely overshadow the practical uses of the technologies. For example, when Google introduced its Buzz social networking platform in winter 2010, the company took advantage of existing patterns of communication in its users' e-mail and instant messaging contact lists. Because Buzz made frequent contacts into shared information by default, the chorus of disapproval from users and privacy advocates forced Google into a protracted cycle of apologies and service adjustments (Helft, 2010).

Theory and Hypotheses: Online Risky Behaviors, Adverse Events, and Social Intelligence

Surfing the Web and communicating with others online involve various levels of uncertainty and risk. Some behaviors are relatively benign, such as exchanging e-mail with friends or reading news on popular, well-known Web sites. Other online behaviors are rife with significant risks. When individuals purchase items on the Web, pay to download digital audio or video, or bid in online auctions, they put tangible assets at risk. In addition, they may reveal sensitive details such as personal contact information, credit card data, or bank account numbers. The frequency with which one engages in online financial transactions constitutes a form of risk-taking with material resources. Many forms of online financial transactions such as direct online purchases, banking, and online auctions are fairly commonplace and have some associated risk. However, we argue that engaging in more frequent online financial transactions implies an acceptance of monetary risk. Although many individuals intermittently engage in online financial transactions, a higher frequency of these behaviors is indicative of both familiarity and a level of comfort with using online tools and systems to exchange money for goods and services.

At first glance, the propensity to take risks might seem like a form of gullibility or naïveté. On the contrary, individuals who frequently engage in risk-taking behaviors develop first-hand experience and tend to make more prudent decisions than those who typically avoid risky interactions (Yamagishi, 2001; Yamagishi, Kikuchi, & Kosugi, 1999). An equally valid possibility is that individuals who proactively engage in discretionary online behaviors may feel comfortable frequently participating in potentially risky financial behaviors. In both cases, our prediction is the same: We expect higher frequency of online financial transactions to positively associate with judicious and prudent online behavior (Web discretion).

> **Hypothesis 1a:** Ceteris paribus, higher frequency of online financial transactions is positively associated with Web discretion.

The experience that comes with greater risk-taking could lead to greater learned pragmatism regarding one's lack of control over personal online information. However, the converse could lead to the opposite prediction. Disregarding other factors, the less control one perceives over her online information, the less likely she is to purposely engage in an increased number of potentially risky online financial transactions. However, if we control for other key factors such as one's self-described information technology knowledge, it follows that a low perception of Web information control would not necessarily be associated with a decrease in financial transactions because the individual is cognizant of the risks involved. Holding information technology knowledge constant, we expect more frequent online financial transactions to negatively associate with perceptions of Web information control.

> **Hypothesis 1b:** Ceteris paribus, higher frequency of online financial transactions is negatively associated with perceptions of Web information control.

Although online financial transactions involve explicit pecuniary risks, other online behaviors entail less specific hazards. For example, individuals who produce and share digital information on Web pages and blogs confront social risks (e.g., critique and derision) as well as potential legal ramifications (e.g., licensing rights and unlawful reproduction of material). Individuals who frequently engage in online creative production are regularly exposed to various types of risk, yet continue to create content and share it with others. As we argue above, frequent participation in risky and uncertain interactions can generate both experience and knowledge about how to protect oneself online. The reverse relationship is similar, as one who actively engages in greater discretionary behaviors may feel more at ease with increased production and sharing of digital information Though the associated risks are different than those in online financial transactions, we expect higher frequency of online creative production and sharing activities to positively associate with Web discretion behavior.

DOI: 10.1002/asi

Hypothesis 2a: Ceteris paribus, higher frequency of online creative production and sharing is positively associated with Web discretion.

Following the same logic above, we might assume that those who regularly produce content on the Web are more knowledgeable about the difficulties associated with controlling personal information online. However, there is a key difference between financial risk-taking and online content production: Individuals who frequently produce and share information in Web pages and blogs are directly and indirectly managing aspects of their own online information and identity. Consequently, it follows that a greater incidence of online creative production and sharing should be positively associated with one's perception of Web information control.

Hypothesis 2b: Ceteris paribus, higher frequency of online creative production and sharing is positively associated with perceptions of Web information control.

Negative experiences are an important part of learning about risk and uncertainty in online or offline settings. Damaging experiences from spam, phishing attacks, identity theft, data loss, viruses, and malware can negatively affect one's online experience and engender a higher awareness of risk. Adverse events can range from harmless and annoying affairs to malicious experiences with potentially detrimental outcomes (Preece, 2004). In part, these problems are our own making because online safety depends on our capacity and motivation to protect ourselves from harm (LaRose, Rifon, Liu, & Lee, 2005). Simply being informed about the potential risks of online interaction is important, but information alone is not always enough to change behavior. Ultimately, threats have the potential to discourage safe behavior unless we know individuals' level of perceived risk (LaRose, Rifon, & Enbody, 2008).

A potentially important indicator of one's heightened perception of risk on the Internet is the experience of an online adverse event. The occurrence of a negative experience makes risks and uncertainties salient to individuals by forcing their involvement. When personal involvement is low, individuals tend to invoke heuristics such as, "relying on the credibility of a web site rather than reading its privacy policy" (LaRose et al., 2008, p. 74). On the other hand, direct involvement brings potential risks to the forefront, leading to proactive behaviors that could protect them from future troubles. In fact, high perceptions of online threats have been shown to strongly associate with safe online behaviors and practices (LaRose et al., 2008).[1] We predict that the experience of an online adverse event will positively associate with Web discretion behaviors. Furthermore, the experience of an adverse event dissuades complacency and serves as a somber reminder that online risks are real. Individuals who experience adverse events should have a greater appreciation for the realities of online risks and uncertainties. The experience of an adverse event should be negatively associated with perceptions of Web information control.

Hypothesis 3a: Ceteris paribus, experience of an online adverse event is positively associated with Web discretion.

Hypothesis 3b: Ceteris paribus, experience of an online adverse event is negatively associated with perceptions of Web information control.

An individual's ability to recognize risky situations with others and to distinguish between trustworthy and untrustworthy individuals is a type of *social intelligence* (Yamagishi, 2001). Counteracting the popular notion that, "those who tend to trust others without hard evidence are easy prey to predators in the social jungle" (Yamagishi et al., 1999, p. 149), Yamagishi (2001) illustrates that individuals who are *less* cautious and *more* trusting of others develop a kind of "street smarts" that improves their ability to identify potentially risky and uncertain social interactions. The explanation for this result is similar to the earlier logic related to the frequency of risky online behaviors and discretionary actions: those who are more trusting in general tend to engage in risky and uncertain environments more often, gaining more experience and opening more opportunities for profitable outcomes compared to less trusting individuals (Cook, Hardin, & Levi, 2005). Hence, generalized attitudes about trusting others in a variety of contexts are likely to associate with attitudes and behaviors in many offline or online interactions. If individuals with higher general trust are likely to gain experience in risky and uncertain situations, it follows that they should be more likely to engage in discretionary behaviors to protect themselves from potential harm, compared to those with less general trust.

Hypothesis 4a: Ceteris paribus, higher general trust is positively associated with Web discretion.

Social intelligence should not be confused with gullibility (Yamagishi et al., 1999). With greater online experience also comes an enhanced knowledge of the pitfalls and challenges of managing information about oneself on the Internet. Individuals with greater social intelligence should possess wisdom and experience to be pragmatic about the dangers of social interactions, allowing them to discern the limitations of their own capabilities in online situations. Hence, individuals with higher general trust should be more likely than those with lower general trust to develop a sense of skepticism about their ability to control their information on the Web, leading to lower perceptions of Web information control.

Hypothesis 4b: Ceteris paribus, higher general trust is negatively associated with perceptions of Web information control.

Yamagishi (2001) argues that individuals with high trust and low caution are more likely to engage in risky but

[1] LaRose et al. (2008) find that high perceptions of risk correlate with safe online behaviors; they also note that the opposite result is found in prior research (e.g., Witte, 1992). The so-called 'boomerang effect' describes the non-linear relationship between fear and prudent behavior. The consensus between the various findings is that threats tend to discourage safe online behavior unless we (1) know something about individual perceptions of risk and, (2) adjust warning notifications to match these perceptions.

DOI: 10.1002/asi

potentially lucrative interactions. However, Yamagishi et al. (1999) find that the *most* socially successful individuals (e.g., those able to make beneficial and productive deals with others) balance higher trust with a healthy measure of caution. In a cross-national study, Yamagishi and Yamagishi (1994) found a triangular shape between the two factors of general trust and general caution. Those with low general trust tend to be highly cautious, but the reverse is not necessarily true. A sizable number of individuals (above 40% in their sample) were highly trusting but also highly cautious. Yamagishi et al. (1999) argue that these results, "suggest that being prudent or cautious in dealing with others does not necessarily imply that a person is distrustful of others in general" (p. 148). It is this unique combination of high trust and high caution that leads some individuals to engage in risky and uncertain social interactions while maintaining a sense of vigilance and discretion (Gordon, 2007; Markoczy, 2003; Yamagishi et al., 1999). As Gordon (2007) argues, trust is the basis for interpersonal interaction and, "balanced dispositions to trust and vigilance should... most benefit the exchange of information" (p. 46). Due to their heightened sense of vigilance, we expect those with higher levels of general caution to indicate higher degrees of Web discretion. However, increased vigilance should also stimulate skepticism and prudence about one's control over personal online information. As with higher trust (Hypothesis 4b), we expect higher general caution to negatively associate with Web information control.

Hypothesis 5a: Ceteris paribus, higher general caution is positively associated with Web discretion.

Hypothesis 5b: Ceteris paribus, higher general caution is negatively associated with perceptions of Web information control.

Methodology: Survey of Internet Behaviors, Experiences, and Attitudes

Materials

To test our hypotheses, we created a Web-based survey instrument that included questions in three primary areas: sociodemographic characteristics, frequency of online activities, and attitudes/dispositions. The survey was built and distributed online using LimeSurvey, a PHP-based open source survey tool.[2] This system provided us with comprehensive control of survey presentation, implementation, and deployment. In addition, we were able to collect data while ensuring anonymity and confidentiality. We first distributed the survey to a pilot group ($N = 70$) to test the survey tool and gather feedback. The pilot test led to several small changes to question presentation, order, and wording. The final instrument contained 88 questions and took approximately 15 minutes to complete.

[2]http://www.limesurvey.org/

Participants and Procedure

We recruited participants for the survey by posting advertisements on the community volunteer request section of a popular online classified listing service, Craigslist.org, in Atlanta, Georgia and Chicago, Illinois. The community volunteer section of Craigslist is a designated place to request participation for surveys, clinical trials, nonprofit activities, and other volunteer work. Our survey participation request indicated that we were interested in learning more about Internet use and attitudes, and that we would offer $5 gift cards to a popular online retailer to the first 200 participants who successfully completed the survey over the next 5 days. Our solicitation did not guarantee payment for participation, and was designed to both pique interest in the topic and to provide the potential for a small financial gift.

As with many participation requests that offer potential gift cards, our survey request was reposted to Web sites that aggregate online survey and research opportunities drawn from many sources, including Craigslist.org. Importantly, all individuals who found our request for participation on Craigslist.org or another site were directed to the same study information page and consent form hosted on our research Web site and server. Thus, our sample is most accurately described as Internet users who are familiar with online classified sites such as Craiglist.org, and are interested in social research or the potential for a $5 gift card. The survey was active for 5 calendar days in July 2008. During this period, 1545 individuals recorded unique entries in our survey database. Of these, 1213 participants fully completed the survey (79% completion rate).

Data Cleaning and Integrity

Researchers have noted that all Internet-based surveys suffer from limitations related to sampling and data integrity (Birnbaum, 2004). Hence, we expected some responses from individuals who rushed through the survey without reading the questions simply to collect the gift card. To identify suspicious responses, we calculated the standard deviation of each participant's responses on each page of the survey.[3] This method allowed us to find respondents who were answering questions with almost the same response every time. Given the many different types of questions on each page (15–20 questions per page) it was extremely unlikely that any participant could provide meaningful answers with little deviation across many different types of questions. Furthermore, several groups of questions included reverse-coded items, so a respondent who answered consistently (e.g., all 1 s or 7 s) would have contradicted herself several times. Forty-eight

[3]As one of our anonymous reviewers notes, another approach to checking data integrity would be an analysis of completion time (assuming that faster completion rates are correlated with poor data responses). Unfortunately, the version of LimeSurvey that we used at the time of data collection did not allow us to record reliable information about start and end times. However, our ability to detect direct contradictions with reverse-coded questions is arguably a very effective way to uncover and flag respondents who were not reading the questions.

TABLE 1. Descriptives for all variables in analyses ($N = 971$).

Variable	*M*	*SD*	Min	Max
Age	32.73	10.48	18	69
Education	3.64	1.23	1	6
Female	0.59	0.49	0	1
IT Knowledge	4.99	1.15	1	7
Financial transactions	2.18	0.98	1	5
Creative production	2.18	1.16	1	5
Adverse events	0.48	0.50	0	1
General trust	4.34	1.09	1	7
General caution	4.42	0.88	1	7
Web discretion	4.65	1.11	1	7
Web information control	3.78	1.52	1	7

Note. Education is reported on the following scale: 1 = Some High School; 2 = High School Graduate; 3 = Some College; 4 = College Graduate; 5 = Some Postgraduate; 6 = Postgraduate.

participants (3.9%) had standard deviations of close to zero for three or more groups of questions and were subsequently flagged for review. After eliminating suspicious data and respondents with 10% missing data or more, the final valid $N = 971$. Means and standard deviations for all variables in the valid sample are displayed in Table 1.

Dependent Variables

Web discretion. Our measure of Web discretion is comprised of 7-point Likert-style agreement statements (1 = *Strongly Disagree*, 2 = *Disagree*, 3 = *Somewhat Disagree*, 4 = *Neither Disagree or Agree*, 5 = *Somewhat Agree*, 6 = *Agree*, 7 = *Strongly Agree*). The Web discretion measure is designed to assess selective, vigilant behaviors that could protect one from harm. We based these questions on related items from the Trust and Privacy Surveys from the Pew Internet & American Life project (www.pewinternet.org). Our Web discretion measure was computed as the average of two positively correlated questions about meticulous and discerning behaviors regarding Web sites and information: "I restrict myself to only Web sites that I trust," and "I carefully read the information I see on the Internet regardless of the Web site it's on" ($r = 0.3$, $p < 0.001$). Figure 1 displays the distribution of Web discretion. The average level of Web discretion in the valid sample is 4.65 with at standard deviation of 1.1.

Web information control. Web information control is the perception that one has control over one's own personal information on the Web. We operationalize Web information control using a direct attitudinal question ("I feel like I don't have control over information about me on the Internet"). This item was based on a question from the 2000 Pew Trust and Privacy survey which dealt with concerns over personal information online. The original Pew question was a simple yes/no response, whereas our version is an agreement statement allowing for greater variation in response. Our question used the same 7-point Likert-style agreement scale described in the Web discretion items above. Because the Web information control question is framed as a negative, we reverse coded the responses so that higher values indicate higher perception of Web information control. Figure 2 displays the distribution of the responses. The average level of Web information control is 3.78, though the standard deviation is rather large, 1.52.

Independent Variables

Online activities. We used scales to measure how often respondents engage in online financial transactions and online content production. These questions were also based on online behavior items from the Pew Internet & American Life Project. However, we asked about frequency of the

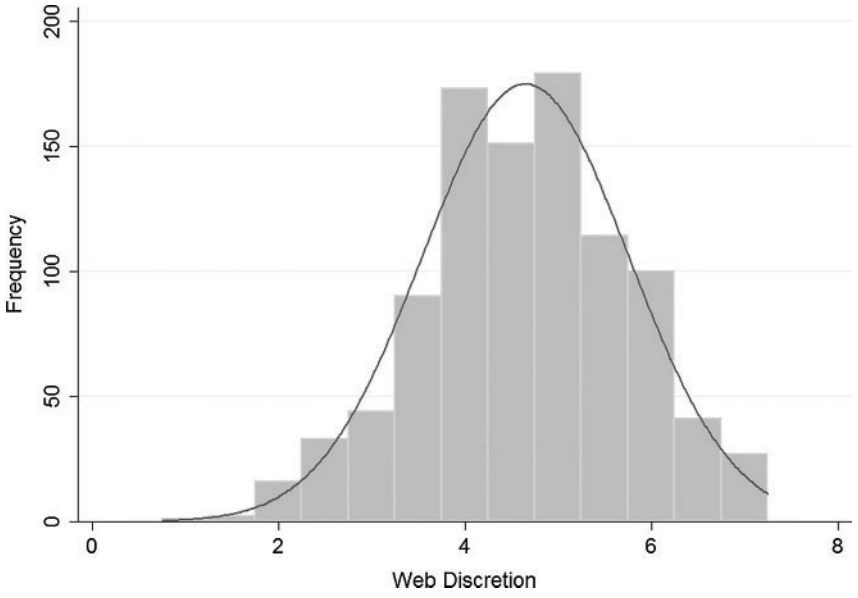

FIG. 1. Frequency distribution of Web discretion.

DOI: 10.1002/asi

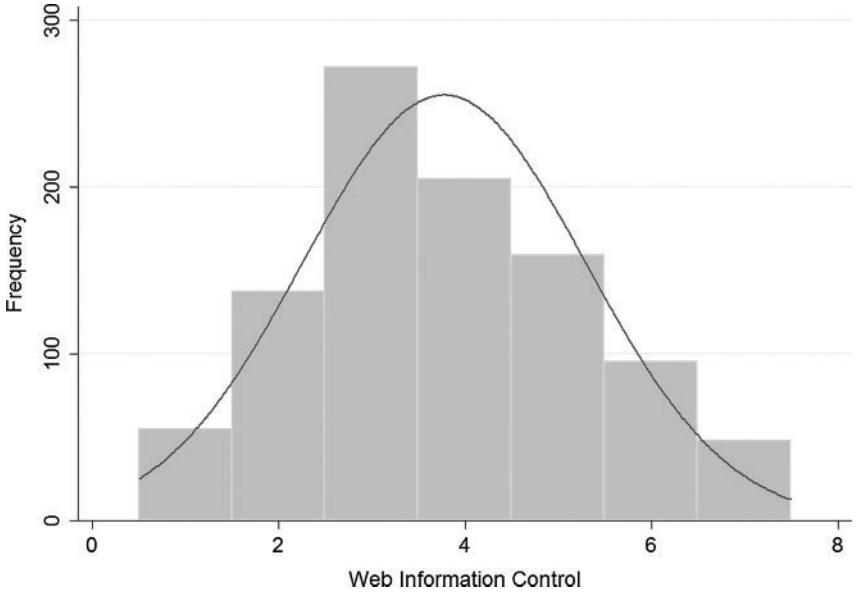

FIG. 2. Frequency distribution of Web information control.

behaviors per week using a 5-item ordinal scale (1 = *Less than once*, 2 = 1–3 *times*, 3 = 4–6 *times*, 4 = 7–9 *times*, 5 = 10 + *times*) rather than dichotomous, yes–no responses like the Pew study. Our scales were created by taking the average of respondents' responses to several related items. The online financial transaction scale included the frequency that the respondent "pays to access or download digital content," "makes a purchase through a Web site," and "participates in an online auction" (Cronbach's $\alpha = 0.77$). The online content production and sharing scale included the frequency that the respondent "shares something online," "works on their own Web page," and "works on their own online journal or blog" (Cronbach's $\alpha = 0.83$). The average activity levels in the sample are on the low end of the scale, 2.18 for both financial transactions and creative production (e.g., 1–3 times per week). Standard deviations for both scales are approximately equal to 1.

Adverse events. The adverse event measure is a dichotomous variable created from a single yes–no response question: "Have you, personally, ever had a bad experience or adverse event on the Internet? An adverse event is any unexpected bad experience in which you, your online accounts, or your computer was attacked or violated in some way that led to a negative consequence (e.g., virus attack, identity theft, password compromise)." As with our other online activity and attitudinal questions, this item was based on similar questions in the Pew Internet & American Life Project. However, the wording of our question was expanded to give both context and examples. As a consistency check, we also collected open-response text about the nature of the adverse event. The open responses were checked for uniformity with the intended concept, and leaned heavily towards virus and worm attacks and password problems on Web sites. In our sample, almost half (48%) of respondents indicated that they had experienced an online adverse event.

General trust and caution. We used Yamagishi's Trust and Caution scales (Yamagishi & Yamagishi, 1994), which have been validated in many diverse studies and continue to be used to measure general trust and caution within and between societies (e.g., Cook, Yamagishi, et al., 2005; Markoczy, 2003; Yamagishi, 2001). Following Yamagishi (1999), we treat the trust and caution scales as indicators of a type of social intelligence—the propensity to trust others and be cautious in social interactions. Consistent with prior research (e.g., Yamagishi & Yamagishi, 1994), the trust and caution scales are negatively correlated ($r = -0.15$, $p < 0.001$).

The trust scale is computed from the average of five items: "Most people are basically honest," "Most people are basically good-natured and kind," "If anything, I trust others," "Most people trust others," and "Most people are trustworthy." Responses range from *Strongly Disagree* to *Strongly Agree* on a 7-point agreement Likert scale (1 = *Strongly Disagree*, 2 = *Disagree*, 3 = *Somewhat Disagree*, 4 = *Neither Disagree or Agree*, 5 = *Somewhat Agree*, 6 = *Agree*, 7 = *Strongly Agree*). The general trust items are highly related (Cronbach's $\alpha = 0.85$). The general caution scale also has five items that are averaged into a single scale (Cronbach's $\alpha = 0.62$). The items include "One can avoid falling into trouble by assuming that all people have a vicious streak," "You cannot be too cautious in dealing with others," "We do not always have to guard ourselves against being used by someone" (reverse coded), "If you are not careful enough, people will take advantage of you," and "It is safer to believe that everyone has the capacity to be malicious." The average general trust and caution responses in the sample are

DOI: 10.1002/asi

near the center of each scale (4.34 and 4.42, respectively). However, the standard deviation for general trust is slightly higher (1.1) than for general caution (0.88).

Sociodemographic Measures and Information Technology Knowledge

Sociodemographic characteristics. Respondents reported their age, gender, and level of education. Age was reported with a free-response text box and gender was a dichotomous choice (male/female) that we recoded into a single variable, female, where 1 = female and 0 = male. Educational level was registered on a 6-item ordinal scale where higher values indicate higher levels of education (1 = *Some High School*, 2 = *High School Graduate*, 3 = *Some College*, 4 = *College Graduate*, 5 = *Some Postgraduate*, and 6 = *Postgraduate Degree*). As Table 1 shows, the average age of our respondents is 33 years, they are 39% female, and the average education level is between some college and college graduate.

Information and technology (IT) knowledge. The IT knowledge scale is designed to measure one's overall level of comfort and self-described knowledge about information technology. This is a crucial control variable in our models because one's self-reported knowledge and confidence with using information technology and systems, "is bounded by our understanding of the conditions under which the technology functions" (Friedman et al., 2000, p. 35). We constructed a measure of IT knowledge from the average of two items: "I fully understand most of the technology I use on a daily basis," and "I usually know enough about the source of online information to decide whether I trust it." As with our other online behavior and attitude items, these questions were based on similar items about technology competence and familiarity from the Pew Internet & American Life Project. Both of our questions use the same 7-point Likert-style agreement statements (1 = *Strongly Disagree*, 2 = *Disagree*, 3 = *Somewhat Disagree*, 4 = *Neither Disagree or Agree*, 5 = *Somewhat Agree*, 6 = *Agree*, 7 = *Strongly Agree*). The two items are highly correlated ($r = 0.46$, $p < 0.001$). The average self-reported IT knowledge in our sample was fairly high (4.99, $SD = 1.15$).

Results

To test our hypotheses we used ordered logistic regression with maximum-likelihood method of estimation. Although our two dependent variables have fairly normal distributions (see Figures 1 and 2), the use of ordinal logistic regression allows us to test associational relationships without assuming that the distances between the levels of our Likert-style responses are equivalent.[4] Table 2 displays the principal bivariate relationships between independent and dependent variables in our analyses. Tables 3 and 4 present the ordered log-odds coefficients (abbreviated as *coef* in text) for each independent variable on Web discretion and Web information control, respectively. The ordered logistic regression results for each dependent factor are presented across four nested models. Model 1 includes only the sociodemographic items and the IT knowledge control variable. The next three models add the key predictor variables in steps: risky online behaviors (Model 2), adverse events (Model 3), and general trust and caution (Model 4). We also include the overall model fit and the change/improvement statistics between each model.

TABLE 2. Bivariate relationships between variables in the analyses ($N = 971$).

	Web discretion	Web information control
Metric variables		
Pairwise correlations		
Age	0.17***	−0.09**
Education	−0.05†	−0.07*
IT Knowledge	0.36***	0.02
Financial transactions	0.08**	−0.02
Creative production	0.09**	0.05†
General trust	0.21***	−0.09**
General caution	0.20***	−0.11***
Dichotomous variables		
Group means comparisons		
Gender		
Male	4.44 (0.05)***	3.77 (0.07)
Female	4.78 (0.04)	3.82 (0.06)
Adverse event		
No	4.66 (0.05)	3.85 (0.07)†
Yes	4.60 (0.05)	3.67 (0.07)

Note. Standard errors are in parentheses.
*$p \leq 0.05$. **$p \leq 0.01$. ***$p \leq 0.001$. †$p \leq 0.1$.

Demographic and Control Variables

The sociodemographic and control variables all show highly significant effects for Web discretion. Older and less-educated respondents indicate higher degrees of Web discretion. We also find positive, significant effects among females and individuals with higher IT knowledge. These effects are consistent across all four models. In fact, one of the strongest effects in any model is the positive association between IT knowledge and Web discretion (*coef* = 0.62, $p \leq 0.001$ in the first three models and 0.53, $p \leq 0.001$ in the fourth model).

The associations between sociodemographic controls and IT knowledge are not quite as clear for Web information control. Age shows a very slight negative effect on Web information control (*coef* = −0.02, $p \leq 0.001$). In addition, education level has a small, negative association with Web information control in the first three models, but given the scale of the variables this is also a very small practical effect. IT knowledge is not significant in the first three models for

[4]For comparison, we also conducted ordinary least squares regression analyses for all models. We find the same significant directional effects for every relationship reported in this article.

DOI: 10.1002/asi

TABLE 3. Web discretion—nested ordinal logistic regression models ($N = 971$).

	Model 1	Model 2	Model 3	Model 4
Age	0.02(0.01)***	0.03(0.00)***	0.03(0.01)***	0.02(0.01)***
Education	−0.10(0.05)**	−0.12(0.05)**	−0.12(0.05)**	−0.13(0.05)**
Female	0.39(0.12)***	0.43(0.12)***	0.43(0.12)***	0.40(0.12)***
IT Knowledge	0.62(0.05)***	0.62(0.05)***	0.62(0.05)***	0.53(0.06)***
Financial transactions		0.19(0.07)**	0.19(0.07)**	0.17(0.07)**
Creative production		0.06(0.06)	0.06(0.06)	0.03(0.06)
Adverse events			0.01(0.11)	−0.02(0.11)
General trust				0.29(0.06)***
General caution				0.40(0.07)***
Log likelihood	−2040.84	−2033.06	−2033.03	−2009.64
Likelihood ratio $\chi 2$	172.08***	187.63***	187.64***	234.47***
Pseudo $R2$	0.04	0.04	0.04	0.06
Model improvement $\chi 2$	167.73***	15.56***	0.01	46.22***

Note. Coefficients are ordered log-odds, with standard errors in parentheses.
*$p \leq 0.05$. **$p \leq 0.01$. ***$p \leq 0.001$.

TABLE 4. Web information control—nested ordinal logistic regression models ($N = 971$).

	Model 1	Model 2	Model 3	Model 4
Age	−0.02(0.01)***	−0.02(0.01)**	−0.02(0.01)**	−0.01(0.01)*
Education	−0.08(0.05)†	−0.08(0.05)†	−0.07(0.05)†	−0.07(0.05)
Female	0.06(0.12)	0.02(0.12)	0.01(0.12)	0.05(0.12)
IT Knowledge	0.00(0.05)	−0.00(0.05)	−0.01(0.05)	0.10(0.06)†
Financial transactions		−0.14(0.07)*	−0.15(0.07)*	−0.14(0.07)*
Creative production		0.13(0.06)*	0.14(0.06)*	0.18(0.06)**
Adverse events			−0.22(0.11)*	−0.19(0.12)†
General trust				−0.25(0.06)***
General caution				−0.35(0.07)***
Log likelihood	−1736.33	−1733.63	−1731.73	−1714.42
Likelihood ratio $\chi 2$	15.39**	20.79**	24.60***	59.21***
Pseudo $R2$	0.00	0.01	0.01	0.02
Model improvement $\chi 2$	15.41**	5.38†	3.81*	34.38***

Note. Coefficients are ordered log-odds, with standard errors in parentheses.
*$p \leq 0.05$. **$p \leq 0.01$. ***$p \leq 0.001$. †$p \leq 0.1$.

Web information control, but it does show a positive, borderline significant effect in the fourth model ($coef = 0.1$, $p \leq 0.1$). Thus, once we control for the effects of general trust and caution, greater IT knowledge is associated with higher perceptions of Web information control. In sum, there are clear sociodemographic and IT knowledge associations with Web discretion, but few with Web information control.

Risky Behaviors

Our first set of hypotheses predicts that the frequency of online financial transactions will be positively associated with Web discretion and negatively associated with Web information control, respectively. Model 2 in Tables 3 and 4 show that frequency of financial transactions is positively associated with Web discretion ($coef = 0.19$, $p \leq 0.01$), and negatively associated with Web information control ($coef = -0.14$, $p \leq 0.05$). The significant effects for financial transactions are sustained in the subsequent models for each analysis. Hypotheses 1a and 1b are supported.

Hypotheses 2a and 2b predict positive associations between frequency of online creative production and the two dependent variables. There is no significant relationship between frequency of creative production and Web discretion in any of the models. However, frequency of creative production has a clear, positive association with Web information control in Model 2 ($coef = 0.13$, $p \leq 0.05$), which persists across all models. Hypothesis 2a is not supported and Hypothesis 2b is supported.

Adverse Events

We argue that the experience of an online adverse event can stimulate a heightened perception of danger and peril on the Internet. We expect those who have had at least one online adverse event to display higher levels of Web discretion and lower levels of Web information control. Surprisingly, adverse events have no significant effect on Web discretion. On the other hand, Model 3 (Table 4) shows that the experience of an adverse event does have a significant,

DOI: 10.1002/asi

negative association with perceptions of Web information control ($coef = -0.22,\ p \leq 0.05$). The coefficient indicates a considerable practical effect, but drops to borderline statistical significance in Model 4 when we control for general trust and caution. Hypothesis 3a is not supported and Hypothesis 3b is supported.

General Trust and Caution

As indicators of a type of social intelligence, we predict that general trust and caution will be positively associated with Web discretion and negatively associated with perceptions of Web information control. Model 4 in Tables 3 and 4 reveals that general trust is positively associated with Web discretion ($coef = 0.29,\ p \leq 0.001$) and negatively associated with Web information control ($\beta = -0.25,\ p \leq 0.001$). General caution displays the same pattern with Web discretion ($coef = 0.40\ \ p \leq 0.001$) and Web information control ($coef = -0.35,\ p \leq 0.001$). Although our purpose is to test specific independent associations on Web discretion and Web information control rather than to construct the highest possible model fit, it is worth noting that the fourth model in each set of nested regressions significantly improves overall fit. Hypotheses 4a, 4b, 5a, and 5b are all supported.

Discussion

The aphorism "The better part of valour is discretion" is often attributed to William Shakespeare's Falstaff in *Henry IV* (Shakespeare, 1597). This phrase is used to justify actions ranging from cowardice, such as Falstaff's rationalization of his own inaction, to situational selectivity in real-world military engagements (Collins, 2001). However, the original 4th century Greek translation simply states, "bravery consists in foresight" (Speake, 2003). It is with some irony, then, that this classic maxim effectively encapsulates the contemporary human dilemma in online environments. Taking advantage of potentially rewarding online environments requires proactive behavior—we must learn how to recognize online risks and act to protect ourselves in the presence of uncertainty.

The objective of this study was to investigate the associations between self-reported online behaviors, experiences, and dispositions and two key outcomes: Web discretion behaviors and perceptions of control over one's own online information. Of our 10 hypotheses, eight received support. Our first set of arguments deal with the association between frequency of risky online activities such as financial transactions and online creative production with Web discretion and information control. More than almost any other behavior, online financial transactions involve the potential for clear, tangible loss. Actively engaging with this risk, however, appears to coincide with the development of discretionary behaviors. Managing money online or participating in auctions provides first-hand experience with a broad array of agreeable and unscrupulous practices. Familiarity with the entire range of behaviors helps individuals to recognize the differences between more or less risky and uncertain exchanges. In fact, individuals who recognize online risks still choose to participate in e-commerce transactions (Corbitt et al., 2003). Our results suggest that the resolve of online consumers to continue engaging in risky financial transactions is not likely due to naïveté. Instead, we find that frequent online transaction activities are associated with online prudence and discretion.

The second risky online behavior we examine in our study is online content creation and sharing. Unlike financial transactions, sharing and producing digital content involve less-specific risks, ranging from personal (e.g., derogatory comments on a blog) to legal (e.g., copyright infringement from remixing and sharing licensed digital content). We do not find any association between online content production and Web discretion behaviors in any of our models. This indicates that the wide variety of potential risks in online content creation and sharing do not translate into more or less prudent Internet practices such visiting only trusted Web sites or carefully reading information online. On the other hand, the significant, positive relationship between online creative production and Web information control suggests that actively producing and sharing content can be a source of individual empowerment. In many ways this was the early promise of Web 2.0 services and technologies: to turn passive consumers into active producers of information and media, and in doing so, allowing them to assume ownership and control over Internet information (Jenkins, 2008). Of course, it remains to be seen whether self-reported information control translates to actual ability or if it is only a perceived illusion. Regardless, those who frequently create and share online content are at the center of the movement to publicly engage the means of information production.

A surprising finding in our study is the limited effect of experiencing an online adverse event. A single unpleasant online experience has the potential to heighten vigilance and awareness by realizing risks and dangers. However, we found that the experience of an adverse event was not significantly associated with Web discretion, though it does show a strong association with Web information control. In light of current research on experiences of online risks and behavior, the relative inconsequentiality of an adverse event for Web discretion may not be that unexpected after all. For example, frequency of virus-related incidents does not translate to more protective behaviors such as the use of antivirus software (Bagchi & Udo, 2003). Furthermore, Brown and Muchira (2004) find that individuals who experience unauthorized use of their personal data for secondary purposes do not significantly change their online purchasing behaviors. However, one factor that does appear to directly affect future behavior is the immediate invasion of privacy through direct marketing techniques (Brown & Muchira, 2004).[5] Thus, it is very likely that our single measure of adverse online events

[5]Incidentally, the results of Brown and Muchira's (2004) study lead to an important, yet woefully unrealized implication: "Spam e-mail is unlikely to be very effective" (p. 68).

DOI: 10.1002/asi

was not granular enough to detect differences that likely exist between different types of negative events. Our free-response questions captured some of this information, but many respondents skipped these open questions or provided very limited contextual information beyond vague descriptors such as, "Adware attack," "Ebay being ripped off [*sic*]," or "Fraud." It is clear that a more nuanced investigation of online adverse events is essential to future studies of Internet experiences, attitudes, and behaviors.

Higher general trust and caution were both strongly associated with increased Web discretion. Web discretion captures an individual's attempts to be prudent and cautious in their navigation of Web sites and online information more broadly. Thus, our results clearly support Yamagishi's (2001; Yamagishi et al., 1999) assertion that more trusting individuals are not necessarily naïve, gullible or inexperienced. In fact, these individuals may be the precise opposite—more experienced but also more prudent as a function of their familiarity with different sources of uncertainty and risk. Our findings are consistent with related research that shows that trust and caution are independent dimensions of a similar concept. The distinctive pattern of higher trust and higher caution indicates a propensity to engage in risky and uncertain social interactions while sustaining forethought and discretion (Gordon, 2007; Markoczy, 2003; Yamagishi et al., 1999). Although prior work on general trust and caution primarily focuses on offline networks and environments, our research demonstrates the associations between general trust, caution, and prudent behaviors equally apply to the online world.

We found strong negative relationships between general trust, general caution, and Web information control. Initially, our argument and findings might seem contrary to both conventional wisdom and earlier research on trusting beliefs and perceptions of online risk. Malhotra et al. (2004) argue that the more an individual trusts an online service (such as a firm), the less likely he or she is to anticipate risks associated with providing personal information to that organization. However, the crucial difference between this earlier work and our finding is that we are not measuring trust in specific organizations. Rather, general trust and caution in our study capture broad dispositions to trust or to be cautious across a range of situations. For this reason, generalized trust is more closely aligned with optimism and risk acceptance rather than direct, relational trust (Hardin, 2002). Malhotra et al.'s (2004) findings show that specific trust in an organization makes one vulnerable to potential risk. In contrast, our findings demonstrate that individuals with higher general trust and caution tend to perceive less control over their online information as a function of greater acceptance of risk coupled with a sense of prudence.

In addition to our primary hypotheses, our results also present several noteworthy associations between the control factors and our two dependent variables. Chief among these effects is the role of IT knowledge. Individuals who self-reported as more knowledgeable about IT were more likely to indicate higher levels of Web discretion. Thus, our results support Friedman et al.'s (2000) argument that building competence and an understanding of Internet risks is connected to individuals' degree of knowledge about the underlying technologies and systems. However, greater self-reported IT knowledge was only significantly associated with Web information control once we accounted for the effects of general trust and caution (social intelligence). The positive association between IT knowledge and Web discretion complements earlier predictions that those with higher levels of Internet and technology proficiencies tend to be attuned to issues of online privacy and security (Hoffman, Novak, & Peralta, 1999). Those with more IT knowledge may indeed have negative perceptions of privacy. Our findings demonstrate that, net of other factors, these individuals are also more likely to believe that they can do something about these concerns.

Finally, we find that gender is strongly associated with Web discretion: women in our sample express significantly higher Web discretion compared to men. However, we did not find a significant association between gender and Web information control. Prior research finds that women tend to perceive a higher level of risk online compared to men, but that personal recommendations lead to greater reductions in perceptions of risk compared to men (Garbarino & Strahilevitz, 2004). In addition, women in the Garbarino and Strahilevitz (2004) study were more willing to act selectively when they were provided with information from which to base their choices. Our results reaffirm this finding, though in a slightly different situation. The significant association between being female and higher Web discretion suggests a broader tendency among women to manage online risks and uncertainties through selective behavior.

Limitations

There are several important limitations of this research. In addition to the nonspecificity of our adverse events measure described above, many of our independent and dependent variables are based on a restricted set of attitudinal agreement statements. Even though our measures are based on the growing set of behavioral and attitudinal questions used in large projects such as the Pew & Internet Life study, there is ample room for improvement in terms of creating valid and reliable measures of Web discretion and Web information control.

Our use of online classified advertising space to recruit active Internet users presents a double-edged sword for our research. The advantage of this recruitment effort is that we want to recruit individuals who actively use the Internet and have at least some basic level of familiarity with the Web. This is certainly not a trivial issue. Although recent data shows that nearly 75% of Americans 18 or older are using the Internet (Lenhart, Purcell, Smith, & Zickuhr, 2010), the most recent available data also suggests that Internet use and broadband penetration are inconsistent across the United States (Spooner, 2003). A disadvantage of sampling from online classified boards (such as Craiglist.org) is the inability to get a truly random sample within the larger sampling

frame of active Internet users. In addition, our recruitment of participants from online classified spaces could mean that we are disproportionally more likely to find individuals who are low on Web discretion. Fortunately, the normal distribution of Web discretion in our sample (Figure 1) provides a good indication that we successfully obtained a varied sample, despite our recruitment limitations. Although our results may not generalize to *all* Internet users, they do provide compelling evidence that online discretion and information control are important concepts that warrant further investigation with larger and more diverse samples. In many ways, the strongest effects in our study are all the more remarkable given the limits of online recruitment and sampling.

Finally, it is important to restate that although our statistical methods and the terminology of these methods might seem to imply causal relationships, our arguments and hypotheses are strictly *associational*. Of course, this is a limitation of all cross-sectional surveys of attitudes and behaviors. There is no way to accurately establish time order and we do not make any causal claims in this research. Furthermore, statistical methods such as regression help establish associations, but not directional causality (despite the sometimes deceptive terminology of independent and dependent factors). As we have previously argued, there is almost certainly a reciprocal relationship between discretionary behaviors and risky behaviors. Individuals learn to act with discretion based on prior experience, and future decisions are influenced by discretionary behaviors. The same logic applies to attitudes about Web information control. The critical point is that causal relationships are best examined through longitudinal surveys and controlled laboratory experiments. The research reported here is the necessary first step, and the strong associations in this research implore us to further investigate the antecedents and impediments to online discretion and information control.

Implications and Conclusion

Our findings have a variety of implications for both theory and practice. First, our research demonstrates that the frequencies with which individuals engage in risky online activities and behaviors are essential to our understanding of online discretion and information control. Online financial transactions are very common as a general category of behavior—but those who frequently engage in such activities also tend to have a greater sense of Internet discretion than those who are less inclined to use the Internet for financial exchange.

The ubiquity of content production and participatory media sharing raises significant issues regarding the democratization of knowledge and what it means to be an amateur or an expert (Rooney, McKenna, & Breit, 2008). As the line blurs between recreational participation and professional content producer, our findings suggest that developers of online systems could do well to embrace and empower those who write product reviews, edit content, and engage in other forms of participation. Our findings imply that online creative production activities such as blogging, editing *Wikipedia*, or posting home-made videos to YouTube are empowering to one's sense of Web information control. Those who frequently create and share online content believe that they have a greater sense of jurisdiction over their own online information, independent of the effects of greater IT knowledge, adverse events, general trust, and caution. Above and beyond the benefits to skill-building and social interaction, creative production and sharing on the Internet allows individuals to participate in their own online identity development and maintenance.

Negative online experiences do not appear to be strongly associated with the propensity to engage in online prudent behaviors. Furthermore, adverse events are not especially damaging to individuals perception of Web information control—the effect is clear, but it is largely overshadowed by other attitudes such as general trust and caution. The popular wisdom is often that a single bad experience can sour all online interactions, potentially driving an affected individual away from new technologies and services entirely. However, our results reveal that one's experience of an adverse online event (as a broad category) is less important for online discretion than other behaviors and predispositions. So, the notion that a single bad experience is enough to drive away users for good may be unfounded. Although the long-term effects of adverse events remains unknown, our results suggest that designers and practitioners of online services do not have to worry so much about the behavioral consequences of a few negative experiences. Frequency of engaging in risky online behaviors and predispositions to engage in risky and uncertain situations are far more important issues for understanding online prudence and beliefs about personal information control.

As a function of general dispositions to trust and be cautious, social intelligence is critical to prudent Internet behavior. Together, Web discretion and Web information control might be the backbone of a different type of "online social intelligence." Just as individuals who are more trusting and prudent are well equipped to handle various offline social interactions, those who are broadly cognizant of risks and uncertainties are also among the best equipped to handle risky online interactions. As one might presume, those who are less cautious in general also tend to report lower Web discretion. However, controlling for other factors, those who are less trusting in general are actually *less vigilant in their self-reported online behavior*. This result might be counterintuitive to designers and practitioners who implicitly assume that those who trust others less are, by definition, more prudent. According to Yamagishi and his colleagues' (1999, 2001) arguments, and further supported by this research, trust and caution are two independent dimensions of a larger construct.

Some might be tempted to infer that a strategy for encouraging and maintaining positive behaviors, attitudes, and online competencies is to instruct Internet users about the benefits of Web discretion. However, our research indicates that we should be targeting the *least* trusting individuals to

DOI: 10.1002/asi

raise awareness and encourage diligent Internet behaviors. The unfortunate paradox is that a key aspect of Web discretion is one's tendency to carefully read information that is presented on the Internet. Less trusting and less cautious individuals are also less likely to be reading about "best practices" and "frequently asked questions" in the first place. Thus, our final implication is that online systems require creative solutions that can access those who are essentially not looking for assistance. Specifically, we cannot expect all individuals to seek out information about how to help themselves from potential online dangers. Instead, we believe that a reasonable alternative is to use behavioral targeting to reach those who are likely to have—or actively demonstrate—lower Web discretion. In much the same way that search companies such as Google, Microsoft, and Yahoo! target advertisements based on prior behavior and content consumption, helpful information about prudent online behavior could be aimed at users based on behavioral patterns of information sharing and Web activities. Of course, there is often a fine line between behavioral targeting and privacy. The key is providing useful information to the user, rather than collecting and sharing information about the user. Assuming that privacy and security can be maintained in a transparent manner, behavioral targeting could be an extremely effective way to directly reach those who could be putting their personal information and identity at risk. Ultimately, helping individuals learn to discriminate in their online interactions can better prepare them to deal with uncertainty on the Internet, and potentially minimize the harmful effects of negative online experiences when and if they occur.

References

Bagchi, K., & Udo, G. (2003). An analysis of the growth of computer and Internet security breaches. Communications of the Association for Information Systems, 12(46), 1–29.

Bargh, J.A., & McKenna, K. (2004). The Internet and social life. Annual Review of Psychology, 55(1), 573–590.

Beatty, S. (1996, February 12). Consumer privacy on the Internet goes public. The Wall Street Journal.

Birnbaum, M. (2004). Human research and data collection on the Internet. Annual Review of Psychology, 55, 803–832.

Brown, M., & Muchira, R. (2004). Investigating the relationship between Internet privacy concerns and online purchasing behaviour. Journal of Electronic Commerce Research, 5(1), 62–70.

Burke, R.R. (2002). Technology and the customer interface: What consumers want in the physical and virtual store. Journal of the Academy of Marketing Science, 30(4), 411–432.

Burkhalter, B. (1999). Race online: Discovering racial identity in Usenet discussion. In M. Smith & P. Kollock (Eds.), Communities in cyberspace (pp. 60–75). London: Routledge.

Caudill, E.M., & Murphy, P.E. (2000). Consumer online privacy: Legal and ethical issues. Journal of Public Policy & Marketing, 19(1), 7–19.

Chen, K., & Rea, A. (2004). Protecting personal information online: A survey of user privacy and control techniques. Journal of Computer Information Systems, 44(4), 85–92.

Cheshire, C., & Cook, K. (2004). The emergence of trust networks: Implications for online interaction. Analyse and Kritik, 26, 220–240.

Cheung, C.M., & Lee, M.K. (2006). Understanding consumer trust in Internet shopping: A multidisciplinary approach. Journal of the American Society for Information Science and Technology, 57(4), 479–492.

Collins, J.M. (2001). Military strategy: Principles, practices, and historical perspectives. Herndon, VA: Potomac Books Inc.

Cook, K.S., Hardin, R., & Levi, M. (2005). Cooperation without trust? New York: Russell Sage Publications.

Cook, K.S., Yamagishi, T., Cheshire, C., Cooper, R., Matsuda, M., & Mashima, R. (2005). Trust building via risk taking: A cross-societal experiment. Social Psychology Quarterly, 68(2), 121–142.

Corbitt, B.J., Thanasankit, T., & Yi, H. (2003). Trust and e-commerce: A study of consumer perceptions. Electronic Commerce Research and Applications, 2(3), 203–215.

DiMaggio, P., Hargittai, E., Neuman, W.R., & Robinson, J.P. (2001). Social implications of the Internet. Annual Review of Sociology, 27(1), 307–336.

Fiore, A., & Cheshire, C. (2010). The role of trust in online relationship formation. In D. Latusek & A. Gerbasi (Eds.), Trust and technology in a ubiquitous modern environment: theoretical and methodological perspectives. Hershey, PA: IGI Global.

Fogg, B.J. (2003). Prominence-interpretation theory: Explaining how people assess credibility online. In CHI '03 extended abstracts on human factors in computing systems (pp. 722–723). New York: ACM Press.

Foster, D. (1996). Community and identity in the electronic village. In D. Porter (Ed.), Internet Culture (pp. 23–37). London: Routledge.

Fox, S. (2000). Trust and privacy online: Why Americans want to rewrite the rules. Washington, DC: Pew Internet & American Life Project.

Friedman, B., Kahn, P., & Howe, D. (2000). Trust online. Communications of the ACM, 43(12), 34–40.

Garbarino, E., & Strahilevitz, M. (2004). Gender differences in the perceived risk of buying online and the effects of receiving a site recommendation. Journal of Business Research, 57(7), 768–775.

Gefen, D., Karahanna, E., & Straub, D.W. (2003). Trust and TAM in online shopping: An integrated model. Mis Quarterly, 27(1), 51–90.

Gomez, J., Pinnick, T., & Soltani, A. (2009, July 1). Know privacy. Unpublished master's thesis, School of Information, University of California-Berkeley.

Gordon, S. (2007). Interpersonal trust, vigilance and social networks roles in the process of entrepreneurial opportunity recognition. International Journal of Entrepreneurship and Small Business, 4(5), 564–585.

Grewal, D., Iyer, G., & Levy, M. (2004). Internet retailing: Enablers, limiters and market consequences. Journal of Business Research, 57(7), 703–713.

Gross, B. (2009, November). (Ab)using identifiers: Indiscernibility of identity. Paper presented at the BayCHI Monthly Meeting, Palo Alto, CA.

Hardin, R. (2002). Trust and trustworthiness. New York: Russell Sage Foundation.

Helft, M. (2010, February 15). Anger leads to apology from Google about Buzz. The New York Times. Retrieved February 10, 2010, from http://www.nytimes.com/2010/02/15/technology/internet/15google.html

Hoffman, D.L., Novak, T.P., & Peralta, M. (1999). Building consumer trust online. Communications of the ACM, 42(4), 80–85.

Jenkins, H. (2008). Confessions of an aca/fan: Archives: The moral economy of Web 2.0 (part one). Retrieved October 20, 2009, from http://www.henryjenkins.org/2008/03/the_moral_economy_of_web_20_pa.html

Jones, K. (2008, December 13). Online consumers more guarded in U.S. than in Europe. Information Week. Retrieved Februrary 10, 2010, from http://www.informationweek.com/news/management/showArticle.jhtml?articleID=172301738

Kelton, K., Fleischmann, K.R., & Wallace, W.A. (2008). Trust in digital information. Journal of the American Society for Information Science and Technology, 59(3), 363–374.

Kiesler, S., & Sproull, L. (1997). "Social" human-computer interaction. In Human values and the design of computer technology (pp. 191–199). Stanford, CA: Center for the Study of Language and Information.

Kim, B., & Han, I. (2009). The role of trust belief and its antecedents in a community-driven knowledge environment. Journal of the American Society for Information Science and Technology, 60(5), 1012–1026.

LaRose, R., Rifon, N., & Enbody, R. (2008). Promoting personal responsibility for Internet safety. Communications of the ACM, 51(3), 71–76.

LaRose, R., Rifon, N., Liu, S., & Lee, D. (2005). Understanding online safety behavior: A multivariate model. International Communication Association, 27–30.

Lee, M., & Turban, E. (2001). A trust model for consumer Internet shopping. International Journal of Electronic Commerce, 6(1), 75–91.

Lenhart, A. (2009, October). The democratization of online social networks: A look at the change in demographics of social network users over time. Paper presented at the Association of Internet Reserchers (AoIR) 10.0, Milwaukee, WI. Retrieved February 10, 2010, from http://www.pewinternet.org/Presentations/2009/41–The-Democratization-of-Online-Social-Networks.aspx

Lenhart, A., Purcell, K., Smith, A., & Zickuhr, K. (2010). Social media and young adults. Washington, DC: Pew Internet & American Life Project.

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

Markoczy, L. (2003). Trust but verify: Distinguishing distrust from vigilance (Working Paper). Riverside, CA: University of California Riverside, Anderson Graduate School of Management.

McLeod, C. (2008). Trust. In E. Zalta (Ed.), The Stanford encyclopedia of philosophy (2008 ed.). Stanford, CA: Stanford University.

Milne, G.R., & Culnan, M.J. (2004). Strategies for reducing online privacy risks: Why consumers read (or don't read) online privacy notices. Journal of Interactive Marketing, 18(3), 15–29.

Nissenbaum, H. (2004). Will security enhance trust online, or supplant it? In R. Kramer & K.S. Cook (Eds.), Trust and distrust within organizations: Emerging perspectives, enduring questions (pp. 155–188). New York: Russell Sage Publications.

Oberndorf, S. (1998, August 1). Users remain wary. Multichannel Merchant. Retrieved February 10, 2010, from http://multichannelmerchant.com/news/marketing_users_remain_wary/

O'Brien, J. (1999). Writing in the body. Gender (re)production in online interaction. In M. Smith & P. Kollock (Eds.), Communities in Cyberspace (pp. 75–106). London: Routledge.

Olivero, N., & Lunt, P. (2004). Privacy versus willingness to disclose in e-commerce exchanges: The effect of risk awareness on the relative role of trust and control. Journal of Economic Psychology, 25(2), 243–262.

Perez, S. (2009, June 30). Social network users reportedly concerned about privacy, but behavior says otherwise. Message posted to ReadWriteWeb. Retrieved February 1, 2010, from http://www.readwriteweb.com/archives/social_network_users_concerned_about_privacy.php

Phelps, J., Nowak, G., & Ferrell, E. (2000). Privacy concerns and consumer willingness to provide personal information. Journal of Public Policy & Marketing, 19(1), 27–41.

Preece, J. (2004). Etiquette online: From nice to necessary. Communications of the ACM, 47(4), 56–61.

Ranie, L., & Tancer, B. (2007). Wikipedia users. Washington, DC: Pew Internet & American Life Project.

Read, B. (2006). Think before you share. Chronicle of Higher Education, 52(20), A41.

Rheingold, H. (2000). The virtual community: Homesteading on the electronic frontier (Rev. ed.). Cambridge, MA: The MIT Press.

Rooney, D., McKenna, B., & Breit, R. (2008). The role of media in the knowledge economy. In G. Hearn & D. Rooney (Eds.), Knowledge policy: Challenges for the 21st century (1st ed., pp. 98–105). Cheltenham, UK: Edward Elgar.

Sardar, Z. (1995). alt.civilizations.faq cyberspace as the darker side of the West. Futures, 27(7), 777–794.

Shakespeare, W. (1597). Henry the 4th. Part 1 Act 5, scene 4, lines 115–121.

Shneiderman, B. (2000). Designing trust into online experiences. Communications of the ACM, 43(12), 57–59.

Speake, J. (Ed.). (2003). The Oxford dictionary of proverbs (4th ed.). Oxford, United Kingdom: Oxford University Press.

Spooner, T. (2003). Internet use by region in the U.S. Washington, DC: Pew Internet & American Life Project.

Sterling, B. (2005). Is the Net doomed? PC World. Retrieved February 15, 2010, from http://www.pcworld.com/article/122499/is_the_net_doomed.html

Strickland, L.S., & Hunt, L.E. (2004). Technology, security, and individual privacy: New tools, new threats, and new public perceptions. Journal of the American Society for Information Science and Technology, 56(3), 221–234.

Sullivan, B. (2009, February 20). Didn't you know? Facebook is forever. The Red Tape Chronicles–MSNBC. Retrieved October 20, 2009, from http://redtape.msnbc.com/2009/02/didnt-you-know.html

Turkle, S. (1995). Life on the screen. New York: Touchstone.

Valentine, G., & Holloway, S. (2001). On-line dangers?: Geographies of parents' fears for children's safety in cyberspace. The Professional Geographer, 53(1), 71–83.

Vance, A., Elie-Dit-Cosaque, C., & Straub, D.W. (2008). Examining trust in information technology artifacts: The effects of system quality and culture. Journal of Management Information Systems, 24(4), 73–100.

Walters, C. (2009a, February 15). Facebook's new terms of service: "We can do anything we want with your content. Forever." The Consumerist. Retrieved October 20, 2009, from http://consumerist.com/5150175/facebooks-new-terms-of-service-we-can-do-anything-we-want-with-your-content-forever

Walters, C. (2009b, February 16). Facebook clarifies terms of service: "We do not own your stuff forever." The Consumerist. Retrieved October 20, 2009, from http://consumerist.com/5154745/facebook-clarifies-terms-of-service-we-do-not-own-your-stuff-forever

Wang, Y.D., & Emurian, H.H. (2005). An overview of online trust: Concepts, elements, and implications. Computers in Human Behavior, 21(1), 105–125.

Westin, A. (1967). Privacy and freedom (1st ed.). New York: Atheneum.

Witte, K. (1992). Putting the fear back into fear appeals: The extended parallel process model. Communication Monographs, 59(4), 329–349.

Wolfinbarger, M., & Gilly, M.C. (2001). Shopping online for freedom, control, and fun. California Management Review, 43(2), 34–55.

Wortham, J. (2009, July 2). Facebook to offer new features to allow users to control privacy of information. The New York Times. Retrieved February 15, 2010 from http://www.nytimes.com/2009/07/02/business/02facebook.html?adxnnl7=1&adxnnlx=1255039427-JBlbK4dS/hT2BCL/OErKSQ

Yamagishi, T. (2001). Trust as a form of social intelligence. In K.S. Cook (Ed.), Trust in society (pp. 121–147). New York: Russell Sage Foundation.

Yamagishi, T., Kikuchi, M., & Kosugi, M. (1999). Trust, gullibility, and social intelligence. Asian Journal of Social Psychology, 2(1), 145–161.

Yamagishi, T., & Yamagishi, M. (1994). Trust and commitment in the United States and Japan. Motivation and Emotion, 18(2), 129–166.

DOI: 10.1002/asi