Know Techn Pol (2010) 23:311–331
DOI 10.1007/s12130-010-9116-6

SPECIAL ISSUE

General and Familiar Trust in Websites

Coye Cheshire · Judd Antin · Karen S. Cook · Elizabeth Churchill

Received: 1 May 2010 / Accepted: 12 June 2010 / Published online: 15 September 2010
© The Author(s) 2010. This article is published with open access at Springerlink.com

Abstract When people rely on the web to gather and distribute information, they can build a sense of trust in the websites with which they interact. Understanding the correlates of trust in most websites (general website trust) and trust in websites that one frequently visits (familiar website trust) is crucial for constructing better models of risk perception and online behavior. We conducted an online survey of active Internet users and examined the associations between the two types of web trust and several independent factors: information technology competence, adverse online events, and general dispositions to be trusting or cautious of others. Using a series of nested ordered logistic regression models, we find positive associations between general trust, general caution, and the two types of web trust. The positive effect of information technology competence erases the effect of general caution for general website trust but not for familiar website trust, providing evidence that general trust and self-reported competence are stronger associates of general website trust than broad attitudes about prudence. Finally, the experience of an adverse online event has a strong, negative association with general website trust, but not with familiar website trust. We discuss several implications for online behavior and suggest website policies that can help users make informed decisions about interacting with potentially risky websites.

Keywords Trust · Online interaction · Computer-mediated communication

C. Cheshire (✉)
School of Information, UC Berkeley, 102 South Hall, Berkeley, CA, USA
e-mail: coye@ischool.berkeley.edu

K. S. Cook
Department of Sociology, Stanford University, Stanford, CA, USA

J. Antin · E. Churchill
Yahoo! Research, 4401 Great America Parkway, Santa Clara, CA 95054, USA

1 Introduction

Trust is an essential part of social interaction (Cook et al. 2009a, b). Without the possibility of trust, individuals would be less likely to begin new relationships and it would be more difficult to maintain existing ones. As a result of the recent explosion in online social interaction, questions surrounding trust in web-based systems have moved to center stage. The challenges and opportunities related to building online trust are compelling, in part because of the sheer diversity and ubiquity of online social experiences. Even the most mundane requirements of daily life are increasingly fulfilled on the web. We communicate with friends and family, search for restaurants and movies, pay bills, and shop online. We are captivated and entertained by digital audio, video, and a wide variety of images from a myriad of sources both professional and amateur. In the course of performing these quotidian activities, we are invited to broadcast our experiences and opinions through viral communication channels such as Facebook (an online social networking site) and Twitter (a service for searching and sharing short messages and updates). At the same time, the web has facilitated popular new forms of social collaboration such as the massively distributed creation of an encyclopedia (Wikipedia) or the aggregation of opinions and reviews on everything from movies and music to restaurants, plumbers, doctors, and hotels.

In all of these online interactions, trust is at issue, because in each case, there are risks and uncertainties of various types. Online purchases can put our tangible assets at grave risk, while our reputations are clearly at risk when we share personal expertise and opinions online. The complexity of many online systems also makes uncertainty a central issue. With varying levels of knowledge concerning how systems operate and how our information may be used comes ambiguity about the potential outcomes of our foray into this online world. While the operation of some systems may seem relatively simple and straightforward, a lack of transparency on the part of the designers can create significant uncertainty about other web-based systems with which we interact. Taking a detailed and specific view of trust provides a lens through which we can understand more fully the nature of the risks and uncertainties involved in a world in which the boundaries of our online and offline interactions are blurred.

A lack of trust in online interactions can have serious consequences. When trust is lacking, communication may be less effective, and working relationships may become less fruitful (Olson and Olson 2000a, b). Lack of trust is also cited as one of the most common reasons consumers choose not to purchase from an online retailer (Grabner-Krauter and Kaluscha 2003), fail to integrate web services such as email systems or social networking sites into their daily activities (Harris and Goode 2004), or shy away from online individual relationships and group memberships. The profiles of these risks and uncertainties are not only a function of the characteristics of distinct contexts (e.g., financial transactions vs. personal communications) but also of diverse patterns of use. Some individuals interact infrequently and tenuously with websites, never integrating web-based tools or services into their lives in meaningful ways. Many others, however, form durable relationships with the websites they use on a daily basis. For these individuals, habitual interactions with specific websites can lead them to perceive risks and uncertainties differently and respond to them in unique ways.

In this article, we focus on individual perceptions of trust in websites, or what we call, *web trust*. We examine two distinct types of web trust—*general website trust* and *familiar website trust*—and indicate their significance for online behavior and interaction. To do this, we examine the relationships between sociodemographic characteristics, attitudes, online activity, and the experience of adverse online events with these two types of web trust. Using data from a survey of active Internet users, we test several hypotheses and discuss the implications of our results for behavior, attitudes, and trust in online environments. Finally, we discuss the implications of our findings for policies and practices on the web.

2 Defining Trust

A central problem for building trust is the initial lack of information about the intentions or behavior of others. This deficiency of information generates uncertainty, while the stakes in a given interaction create risk (Cook et al. 2005a, b). Together, risk and uncertainty produce the conditions that bring about the need for trust. If there are no uncertainties or risks, then trust has no real meaning in a situation (Hardin 2002; Luhmann 1979). Trust and trustworthiness are often assumed to have the same meaning, but the two terms are conceptually different. A review of many different definitions across disciplines indicates that trust most often refers to attitudes, dispositions, or beliefs that we have about others whom we hope will be trustworthy (McLeod 2008). The development of trust requires time and experience between parties. On the other hand, trustworthiness usually refers to a property, personality trait, or characteristic of an individual whom we may trust (Cook et al. 2009a, b; McLeod 2008). Trustworthiness is important for determining when trust is warranted (McLeod 2008), and it is often viewed as a precursor to trust because an individual may assess another as trustworthy without any prior interaction. Individuals may rely on socially valued status characteristics (age, occupation, education) to gauge one's trustworthiness when these attributes are associated with higher performance expectations (Cook et al. 2005a: 30).

Some scholars argue that the most accurate uses of the term "trust" should be reserved for interpersonal relationships between humans (Hardin 2002). In his encapsulated-interest view, Hardin argues that trust is much more than an acceptance of risk or cooperation between individuals. Relational trust can only develop over time in a direct relationship, when one party to the relation believes the other party has incentive to act in her interest or to take her interests to heart (Cook et al. 2005a, b; Hardin 2001).

If the encapsulated-interest view of trust were on one end of a continuum of types of interpersonal trust, general trust might be thought of as the other end. General trust refers to an individual's default expectations about the trustworthiness of other people in the absence of a specific context (Rotter 1967; Yamagishi and Yamagishi 1994; Yamagishi 1998). General trust is viewed as a rough accumulation of attitudes and beliefs in multiple contexts and through experience over time (Cook 2001). It is this context-independence that makes general trust difficult to reconcile with interpersonal trust since the latter is intrinsically tied to the circumstances of social interaction (Hardin 2002). Despite its imprecise nature, general trust is consistently and strongly correlated with a variety of other cooperative and trusting behaviors. Researchers have examined general trust as a predisposition for cooperative and pro-

social behaviors in a variety of environments (Yamagishi 1998) and across cultures (Hayashi et al. 1982; Yamagishi and Yamagishi 1994).

High general trust implies a belief in the benevolence of others' intentions, while low general trust indicates an inclination to adopt a guarded, more skeptical view of others (Yamagishi 1998). Importantly, high general trust does not necessarily equate with gullibility (Rotter 1967). In fact, discretion and caution toward others are both highly related to trust, but they are independent concepts (Yamagishi and Yamagishi 1994). Higher general trust is sometimes associated with lower dispositions to be cautious of others, and individuals with high trust and low caution are more likely to engage in a wider variety of risky but potentially profitable and beneficial interactions (Yamagishi 2001). Individuals who are more trusting and less cautious of others open themselves to many potentially rewarding opportunities (Yamagishi 2001). These individuals experience risks that they may not be prepared to handle without a stronger sense of prudence. General trust and caution are not always inversely related, however (Yamagishi and Yamagishi 1994). Many individuals indicate that they are highly trusting but also highly cautious in their interactions with others. Prudence and caution are not necessarily indicative of distrust (Yamagishi et al. 1999). In fact, the combination of high caution and high trust may explain why some individuals engage in social interaction in the presence of different types of uncertainty (e.g., anonymous partners, indeterminate outcomes) while also being discerning of potential threats and remaining attentive to the risks (Gordon 2007; Markoczy 2003; Yamagishi et al. 1999).

3 Trust in Online Contexts

There are many sources of uncertainty and risk in online environments. Monetary, psychological, and interpersonal risks abound when we provide information about ourselves on the Internet. In addition, individuals face uncertainty about the accuracy, credibility, and sources of information shared online (Cheshire et al. 2010). Anonymity and a general lack of interaction cues in online environments can magnify perceptions of uncertainty and risk, making trust essential but also difficult to assess (Kollock 1999).

Despite collective appreciation of the importance of trust in explaining the extent and form of individuals' online participation, consensus on the meaning of trust in specific online interactions has yet to emerge. Online trust has been the focus of a wide variety of research in computer-mediated communication, human–computer interaction, and related fields (Grabner-Krauter and Kaluscha 2003; Olson and Olson 2000a, b; Riegelsberger et al. 2003). However, this literature uses the term "trust" to refer to several related but somewhat distinct concepts that often confuse or conflate many different ideas (Cheshire and Cook 2004; Grabner-Krauter and Kaluscha 2003; Grabner-Krauter et al. 2006). In online contexts, the conflation of trust with related terms such as credibility, security, surety, and reliability has led to a surplus of complex conceptual models at the expense of consistency and clarity in the use of trust-like ideas (Nissenbaum 2004). When notions of trust are poorly or inaccurately defined, we lose the ability to unpack key concepts and examine meaningful determinants and effects. This type of conceptual confusion makes it difficult to relate distinct studies about trust to one another and to identify the most salient findings about behavior across different online and offline contexts of interaction. From a practical point of view, we also lose

the ability to undertake constructive repair when violations of online trust occur in part because we do not know the underlying source of the problem.

One of the major points of contention in the online trust literature is whether notions of trust that describe interpersonal relationships can be similarly applied to relationships with online entities such as websites. Some scholars have argued firmly that "people trust people, not technology" (Friedman et al. 2000). Others have argued the opposite, suggesting that because we tend to anthropomorphize our interactions with applications and information (Nass et al. 1994), we need not make a distinction between interpersonal trust and human–system trust (Marsh and Dibben 2003). Both perspectives have merit, but they may lead to different implications for users, systems, or those who design online systems.

Interpersonal trust largely hinges on the uncertainty and risk that comes from the possibility of betrayal by another individual (Baier 1986; Hardin 2002; McLeod 2008). Websites and most information systems do not choose to betray in an authentic way because they lack agency (Friedman et al. 2000). However, online systems can be unreliable, present false or incomplete information, or be insecure environments for information sharing. Even if an online system is not capable of sentient betrayal, those who build and maintain it are able to influence the actions and behaviors of the system (Bargh and McKenna 2004). Website operators and designers are also accountable for the malfeasance, fraud, and deceit that occur in the context of the systems they manage or design. In this view, an online system is actually a proxy for the decisions and implementations of its designers. Although trust is not truly dyadic[1] between humans and Internet systems or websites, the experience of risk, uncertainty, and even betrayal is arguably very similar to that of interpersonal trust from the perspective of the user. It is for this reason that trust in websites and systems is meaningful to users even if there are important semantic and scholarly distinctions to be made between these concepts.

3.1 Web Trust: General and Familiar Trust in Websites

General trust in the offline social world has a direct analog in the context of interactions with websites. We call an individual's broad, context-independent attitudes about the trustworthiness of typical websites on the Internet *general website trust*. When individuals interact or exchange information using the web as a medium, they are exposed to a variety of uncertainties and risks. Broad based, abstracted dispositions provide a foundation for our assessments of risk and uncertainty on the Internet. General trust attitudes will often be supplemented by individual experience with specific websites over time. In turn, the long-term aggregation of specific experiences may alter general perceptions of website trust. In this way, general website trust forms a key part of an ongoing evolutionary cycle of online experience, attitudes, and behaviors.

[1] Some key components of relational trust include perceptions, risk-taking, experiences, reactions, and interpretations of others' behavior over time (Cook 2001; Hardin 2002). These components are essential for both parties in a given dyad. In interactions with Internet systems and websites, the experience is unilateral: the user faces risk and uncertainty and may modify her behavior based on personal experience or third-party reputations (Cook et al. 2009a, b). Internet systems, however, rarely modify their reactions to risk and uncertainty based on "experience" with specific users over time or do so in extremely limited ways.

Individuals can also develop more specific perceptions about the trustworthiness of the websites and information systems they use on a regular basis. We refer to this type of web trust as *familiar website trust*. Like situational trust (Marsh and Dibben 2003), familiar website trust focuses on a clear circumstance or setting. Perceptions of trust related to websites that are a part of people's daily habits are arguably more circumscribed than for the general category of all websites. These attitudes are not only context specific but also informed by particular histories of contact and established patterns of regular interactions. In order to examine the differences between general and familiar website trust, we analyze them as separate components of the larger concept of web trust.

These two types of web trust are comparable to *system trust*, which exists when a computer or information system is assumed to operate in a predictable or reliable way (Grabner-Krauter and Kaluscha 2003). Thus, general and familiar website trust only deal with the perceptions that individuals develop about websites or systems, not their interpersonal relationships mediated through communication technology. Our use of the term "web trust" is also distinct from the evaluation of specific aspects of websites that affect the believability or authenticity of content. For example, trust in specific website information content such as layout, color schemes, use of photographs, and writing style is more accurately described as web credibility (Fogg et al. 2001; Fogg and Tseng 1999).

4 Hypotheses

We develop five sets of hypotheses about online activity, general trust, general caution, information technology competence, and the experience of an adverse online event on the two types of web trust (general and familiar) we have distinguished. In each case, we hypothesize and subsequently examine these relationships as associational effects. There is no way to accurately establish time order and direct influence in a self-report cross-sectional survey, but a more important issue is that there is unquestionably a reciprocal relationship between behaviors, dispositions, and attitudes about web trust. Behaviors and dispositions influence experiences and vice versa. For both convenience and consistency, our hypotheses frame web trust as an outcome, but it is essential to proper interpretation of our results that we avoid causal inferences at this point and focus on direct associations. In future extensions of our work, we intend to conduct longitudinal research to mitigate this limitation.

When individuals frequently engage in various online activities, they also develop familiarity with those activities. Familiarity is a perception based on knowledge and experience that a given set of situations or interactions are known and understood. When individuals are more familiar with a given situation, transaction, or individual, their perception of uncertainty tends to be lower (Luhmann 1979). As we have argued, uncertainty and risk are essential conditions for the meaningful application of conceptions of trust. Personal experience with a given situation or partner over time has the potential to build trust (Blau 1964). Empirical work supports this effect in online interactions as well. In a study of the users of a large online retailer, familiarity with a specific website was related to increased trust in the retailer, as well as more frequent inquiries about products and a greater number of purchases

(Gefen 2000). Awareness and frequent use of websites have also been shown to be significantly associated with trust in consumer websites in general (Yoon 2002). All other things being equal, we expect higher frequency of online activity to reduce uncertainty through awareness and to be positively associated with the two forms of web trust.

H1.a-b. Ceteris paribus, a higher frequency of online activity is positively associated with higher (a) general website trust and (b) familiar website trust.

General trust is a default set of expectations about the trustworthiness of others (Yamagishi et al. 1999). Those with high general trust assume that most individuals are trustworthy until experience reveals otherwise. So, high general trust reflects an attitude of risk and uncertainty acceptance or a lack of perceived risk and uncertainty (Yamagishi 2001). Those with higher degrees of general trust should be less deterred from engaging in risky or uncertain activities, more prone to try new activities, and more likely to repeat these activities.

Empirical evidence suggests that individuals do behave differently on the Internet depending on their general attitudes about trusting others. For example, Gefen (2000) found that an individual's disposition towards trusting others was a primary factor influencing behavior in online retailer interactions. Similar results have been found for the effect of general trust in online banking (Suh and Han 2002) and consumer trust in E-Commerce systems (Chen and Dhillon 2003). Consistent with this line of research, we expect higher levels of general trust to be positively related to general and familiar website trust.

H2.a-b. Ceteris paribus, higher general trust is positively associated with higher (a) general website trust and (b) familiar website trust.

General trust is often negatively correlated with general caution (Yamagishi and Yamagishi 1994), but the two dispositions tend to operate independently in a variety of contexts. Yamagishi and Yamagishi (1994) find that individuals with low general trust are often highly cautious, but the reverse is not as common. In fact, a significant proportion of individuals tend to be both highly trusting and highly cautious, suggesting that prudence does not imply distrust of others (Yamagishi et al. 1999).

We have already argued that general trust should be positively associated with the two forms of web trust. However, engaging in risky and uncertain situations does not necessarily entail gullibility. Those who engage in risk-taking behaviors also tend to make more careful decisions compared to those who normally avoid risky and uncertain situations (Yamagishi 2001; Yamagishi et al. 1999). High general trust together with high general caution may signify an inclination to engage in risky and uncertain interactions while also maintaining discretion and prudence (Gordon 2007; Markoczy 2003; Yamagishi et al. 1999).

Although general trust tends to vary widely within communities, Yamagishi and his colleagues (Yamagishi et al. 1999; Yamagishi and Yamagishi 1994) have shown that general caution is not only independent from general trust, but that prudence is fairly common among high and low trusters. Furthermore, there is fairly consistent evidence that prudence among Americans has been growing over time, independent of attitudes about trust, benevolence, or other aspects of human nature (Yamagishi et al. 1999). In uncertain and risky environments, it is reasonable to practice discretion

even as one remains open to new opportunities and interactions. Controlling for one's disposition to trust others, we expect general caution to be positively associated with both forms of web trust.

H3.a-b. Ceteris paribus, higher general caution is positively associated with higher (a) general website trust and (b) familiar website trust.

Knowledge of information technologies and systems is tied to one's understanding of the functionality, design, and use of those technologies (Horrigan 2007, p. 35). As one becomes more familiar with web site procedures and design, it can reduce uncertainty and increase one's understanding of Internet situations (Gefen et al. 2003). Individuals who are more proficient with information technology and the Internet tend to recognize threats such as violations of security and privacy (Hoffman et al. 1999). Thus, we argue that higher levels of self-reported information technology competence should positively relate to the two forms of web trust.

H4.a-b. Ceteris paribus, higher levels of information technology competence are positively associated with higher (a) general website trust and (b) familiar website trust.

The experience of an adverse online event is an important problem for web trust. Potentially harmful online events can range from annoying distractions (e.g., spam email) to malicious experiences (e.g. viruses, identity theft) with potentially injurious financial, social and legal outcomes (Preece 2004). Information and knowledge about the potential risks of online interaction is important, but information alone is not always enough to change behavior.

The occurrence of a negative experience highlights the risks and uncertainties surrounding engagement in these activities and can weaken confidence in the security and reliability of a given system. Among scholars and producers of online systems, there is a vision of online trust that Nissenbaum (2001) describes as, "trustworthiness as security, or trust through security" (p.637). In response, a common view among security and information technology specialists is to lock down computer systems to make them as impenetrable as possible to attack in order to increase trust. These attempts to create assurances can increase the perceptions of security, but may also "squeeze trust out of the picture," since trust depends on uncertainty and risk (Nissenbaum 2001, p. 656). Despite differences in opinions about how to address online threats, there is clear agreement about the deleterious effects of adverse events on trust in online systems and environments. The experience of an adverse online event should be negatively associated with both forms of web trust.

H5.a-b. Ceteris paribus, the experience of an adverse online event is negatively associated with higher (a) general website trust and (b) familiar website trust.

5 Methodology

To examine our research hypotheses, we analyzed data from a survey of online behaviors and attitudes. Our web-based survey included questions in four primary

areas: (1) sociodemographic characteristics; (2) frequency of online activity questions; (3) attitudinal questions about general trust and caution; and (4) agreement statements related to website trust.

We managed the creation and distribution of the survey using the open-source survey tool, LimeSurvey. This system provided us with control over the presentation of our survey, while ensuring the anonymity and confidentiality of our respondents. We first distributed the survey to a small convenience sample that served as a pilot test (N=70). The pilot survey led to several small changes in question presentation, ordering and wording. The final instrument contained 88 questions and took approximately 15 min to complete. The final sample size was N=971.

5.1 Sample and Procedure

We recruited participants by posting advertisements for our survey on the community volunteer request section of the popular online classified listing service, Craigslist.org, in Atlanta, Georgia and Chicago, Illinois.[2] Our survey request was also reposted to websites that aggregate online survey and research opportunities drawn from many sources, including Craigslist.org. The survey announcement 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 a 5-day period. The recruitment posting was designed to appeal to those who are interested in social research, while providing the potential for a small financial gift. 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 and/or the potential for a $5 gift card.

The survey was active for five calendar days in July, 2008. During this period, 1,545 individuals recorded unique entries in our survey database. Of these, 1,213 participants fully completed the survey (79% completion rate). To identify suspicious responses (e.g., individuals who attempted to rush through the survey for a chance at a gift card), we calculated the standard deviation of each participant's group of responses on each page of the survey. 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 (approximately 5–15 questions per page), it was 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 1s, 3s or 7s) would have contradicted herself several times. Forty-eight participants (3.9%) had standard deviations 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. Univariate statistics for all variables in our analyses are shown in Table 1.

[2] The community volunteer section of Craigslist is a designated place to request participation for surveys, clinical trials, non-profit activities, and other volunteer work.

Table 1 Descriptive statistics for all variables in analyses

Variable	Mean	SD	Min.	Max.
Age	32.73	10.48	18	69
Education	3.64	1.23	1	6
Female	.59	.49	0	1
Online Activity	2.25	.88	1	5
General Trust	4.34	1.09	1	7
General Caution	4.42	.88	1	7
Adverse Online Events	.48	.50	0	1
IT Knowledge	4.99	1.15	1	7
General Website Trust	4.16	1.36	1	7
Familiar Website Trust	4.84	1.34	1	7

N=971; 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"

5.2 Dependent Variables

General website trust and familiar website trust Our measure of general website trust is a seven-point Likert-style agreement statement, "I think most websites are trustworthy," (1=Strongly Disagree, 2=Disagree, 3=Somewhat Disagree, 4=Neither Disagree or Agree, 5=Somewhat Agree, 6=Agree, 7=Strongly Agree). Familiar website trust is also a single seven-point Likert-style agreement statement, "I find it easy to trust websites that I use on a daily basis." This question uses the same ordered categories listed above. These measures for general website trust and familiar website trust were based on comparable questions from the Trust and Privacy surveys from the Pew Internet & American Life project (www.pewinternet.org). Both measures are ordinal, and the distributions of the ordered responses to each type of web trust question are approximately normally distributed. However, both general website trust (skewness=−.22) and familiar website trust (skewness=−.56) are slightly negatively skewed. The distributions of our two dependent variables indicate sufficient variation within our online sample.

5.3 Independent Variables

General trust and caution We measured general trust and caution using Yamagishi's scale (Yamagishi and Yamagishi 1994). The instrument is comprised of ten agreement statements including five general trust and five general caution items. Yamagishi's scale has been replicated and validated in many diverse studies and continues to be used to measure general trust and caution within and between societies (e.g., Cook et al. 2009a, b; Markoczy 2003; Yamagishi 2001). Consistent with prior research (e.g., Yamagishi and Yamagishi 1994), the trust and caution scales are negatively correlated (r=−.15, p<.001).

The general trust index is computed as 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 the same seven-point Likert-style agreement scale described above. The general trust items are highly related (Cronbach's α=.85).

The general caution scale also has five items that are averaged to create a single index: "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 general caution items are highly related (Cronbach's α=.62).

Adverse events The adverse online 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)." Almost half of our sample indicated that they had experienced at least one adverse online event (48%).

Frequency of online activity Our measure of overall online activity is an index created by averaging the responses of our participants on 20 individual questions in four major groups of online activities: communication (sending instant messages, email), content creation (blogging, posting comments), financial transactions (purchasing, online auction participation), and digital downloading (downloading audio, video and software). The activity scale items asked how often the respondent engaged in each activity in an average week on a five-point ordered scale: (1=Less than once, 2=1-3 times, 3=4–6 times, 4=7–9 times, 5=10+ times). The online activity items are highly related (Cronbach's α=.86).

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. We constructed a measure of IT Knowledge based on the average of the responses to 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." 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 seven-point Likert-style agreement statements described above. The two items are highly correlated (r=.46, p<.001).

Sociodemographic measures Participants in the survey were asked to report their age in years, gender (recoded to a single binary variable called female), and education level on a six-item ordinal scale (1=Some High School, 2=High School

Graduate, 3=Some College, 4=College Graduate, 5=Some Postgraduate, and 6=Post-Graduate Degree).

6 Results

We used ordered logistic regression with the maximum-likelihood method of estimation to test our hypotheses without assuming equal distances between the ordered categories of the two dependent variables. Tables 2 and 3 display the ordered log-odds coefficients for each independent variable on general website trust and familiar website trust, respectively. The results for each table are presented across four nested regression models. Model 1 includes sociodemographic items and online activity. The next three models add key predictor variables in steps: general trust and caution (Model 2), information technology knowledge (Model 3), and the experience of an adverse online event (Model 4). The model fit and improvement statistics are also provided for comparison within each table.

To help illustrate how varying response levels of key variables lead to tangible differences in general and familiar website trust, we used example profiles to create predicted probabilities. The predicted probabilities are created by solving the complete ordered logistic regression equation (model 4 in each regression) for each independent factor. The result is a predicted probability for all ordered categories of general and familiar website trust. Each row of the table gives the probability of the indicated level of the dependent variable, given the value of the key independent variable in the corresponding column. For each column of predicted probabilities,

Table 2 Nested ordinal logistic regression models for general website trust

	Model 1	Model 2	Model 3	Model 4
Age	.02 (.01)***	.01 (.01)†	.01 (.01)*	.01 (.01)*
Education	.05 (.05)	−.01 (.05)	−.01 (.05)	−.01 (.05)
Female	−.04 (.12)	−.12 (.12)	−.15 (.12)	−.16 (.12)
Online Activity	.30 (.07)***	.14 (.07)*	.13 (.07)*	.14 (.07)*
General Trust		.69 (.06)***	.62 (.06)***	.62 (.06)***
General Caution		.19 (.07)**	.10 (.07)	.11 (.07)
IT Knowledge			.29 (.06)***	.28 (.06)***
Adverse Online Events				−.23 (.12) *
Log Likelihood	−1,639.81	−1,575.12	−1,561.77	−1 559.77
Likelihood Ratio χ^2	31.10***	160.47***	187.18***	191.17***
Pseudo *R*2	.00	.04	.06	.06
Model Improvement χ^2	30.68***	124.51***	26.44***	3.99*

N=971; coefficients are ordered log-odds, with standard errors in parentheses

***p<.001, **p<.01, *p<.05, $^{\dagger}p$<.1

Table 3 Nested ordinal logistic regression models for familiar website trust

	Model 1	Model 2	Model 3	Model 4
Age	.01 (.01)**	.00 (.01)	.00 (.01)	.00 (.01)
Education	−.01 (.05)	−.07 (.05)	−.07 (.05)	−.07 (.05)
Female	.17 (.12)	−.08 (.12)	.07 (.12)	.07 (.12)
Online Activity	.04 (.07)	−.14 (.07)*	−.16 (.07)*	−.16 (.07)*
General Trust		.59 (.06)***	.44 (.06)***	.44 (.06)***
General Caution		.41 (.07)***	.23 (.07)**	.22 (.07)**
IT Knowledge			.73 (.06)***	.74 (.06)***
Adverse Online Events				−.06 (.11)
Log Likelihood	−1,600.89	−1,543.87	−1,467.97	−1,467.85
Likelihood Ratio χ^2	8.99†	123.03***	274.82***	275.07***
Pseudo *R*2	.00	.04	.09	.09
Model Improvement χ^2	8.95†	111.82***	144.32***	.25

N=971; coefficients are ordered log-odds, with standard errors in parentheses

***p<.001, **p<.01, *p<.05, $^{\dagger}p$<.1

one variable was held at a theoretically important value (indicated by column heading), while all other values were kept at the median for the sample (See notes in Table 4 for median values). For example, the first two columns in Table 4 show the predicted probabilities for the seven levels of general and familiar website trust when information technology knowledge is high (7) and all of the other variables in the model are held at the median values. The predicted probabilities indicate that individuals with high IT knowledge are much more likely to have higher web trust (y=4, 5, 6, 7) than lower web trust (y=1, 2, 3).

6.1 Online Activity

Hypotheses H1.a and H1.b predict that the frequency of online activity will be positively associated with general website trust and familiar website trust, respectively. Model 1 in Table 2 shows that increasing levels of online activity are positively related to general website trust (*coef.*=.30, p<.001). This effect is sustained across all four models. However, frequency of online activity does not appear to be related to familiar website trust in Model 1 of Table 3 (*coef.*=.04, p=n.s.). In fact, the effect of online activity actually shows a significant negative effect in models 2–4. We explore this surprising finding in the discussion below. Hypothesis 1. a is supported, but H1.b is not supported.

6.2 General Trust and Caution

We predict that general trust and general caution will be positively associated with general website trust (H2.a and H3.a) and familiar website trust (H2.b and H3.b). We find significant positive effects for general trust (*coef.*=.69, p<.001) and for caution

Table 4 Predicted Probabilities for Each Level of General Website Trust (GWT) and Familiar Website Trust (FWT) by Key Independent Variables

	High IT Knowledge (X=7)		High Online Activity (X=7)		High General Trust and Caution (X=7)		Experience of Adverse Online Events (X=1)	
	GWT	FWT	GWT	FWT	GWT	FWT	GWT	FWT
Pr(y=1|x)	.01	.00	.02	.01	.00	.00	.03	.01
Pr(y=2|x)	.04	.01	.04	.04	.01	.01	.07	.03
Pr(y=3|x)	.12	.02	.14	.13	.04	.02	.20	.09
Pr(y=4|x)	.25	.06	.27	.21	.11	.04	.30	.17
Pr(y=5|x)	.37	.29	.36	.41	.34	.24	.29	.43
Pr(y=6|x)	.16	.41	.14	.15	.35	.42	.09	.22
Pr(y=7|x)	.04	.22	.04	.04	.15	.27	.02	.06

All variables other than X for each column are kept at the median values in each set of predicted probabilities (age=33, educ =3.6, female =.59, online activity =2.3, general trust =4.3, general caution= 4.4, IT Knowledge =4.9, adverse online events =.48). Individual probabilities are rounded to two decimal points

GWT General Website Trust; *FWT* Familiar Website Trust

(*coef.*=.19, $p<.01$) on general website trust in Model 2. While this effect is sustained for general trust across all models, general caution is no longer significantly related to general website trust once we control for information technology knowledge (model 3) and the experience of an adverse online event (Model 4). H2.a is fully supported and H3.a is partially supported.

Familiar website trust displays a consistent, significant relationship with general trust and caution. General trust is positively associated with familiar website trust (*coef.*=.59, $p<.001$) in model 2, and this effect is sustained across all models. In addition, general caution is positively associated with familiar website trust (*coef.* =.41, $p<.001$) in model 2 and this effect is also sustained across all models. H2.b and H3.b are supported.

6.3 Information Technology Knowledge

We predict that one's self-reported knowledge about information technology will be positively associated with both forms of website trust. Indeed, information technology knowledge shows a strong, significant association with general website trust (*coef.*=.29, $p<.001$) in model 3. This effect is also preserved in model 4 once we control for the experience of an adverse online event. Information technology knowledge is similarly associated with familiar website trust (*coef.*=.73, $p<.001$) in model 3. As with general website trust, this effect remains in model 4. This is one of the largest overall effects in our models, indicating that self-reported information technology knowledge is extremely strongly associated with both types of website trust, especially familiar website trust. As the probability profiles show (Table 4), the predicted probability that an individual has one of the top three levels of familiar website trust is much higher if they also indicate high information technology knowledge, net of other factors. H4.a and H4.b are supported.

6.4 Experience of an Adverse Online Event

Our last two hypotheses predict that the experience of an adverse online event will be negatively associated with the two forms of website trust. The fourth model in each set of ordered logistic regressions indicates that adverse events are significantly associated with general website trust (*coef.*=.−.23, $p<.05$). Interestingly, there is no significant effect for adverse events on familiar website trust (*coef.*=−.06, p=ns). This is an interesting finding, as it may indicate that adverse online events can hamper one's general sense of website trustworthiness, without affecting the sense of trust one has for their circumscribed set of familiar websites. H5.a is supported, but H5.b is not supported.

7 Discussion

In this research, we have focused on general website trust and familiar website trust as two distinct forms of web trust. One of our key arguments is that familiarity with online systems through increased activity is an important part of reducing perceptions of uncertainty in online environments. We found the expected positive relationship between online activity and general website trust, supporting the argument that experience with web-based systems is part of a reciprocal cycle of online activity and general website trust. However, we did not find the predicted relationship between online activity and familiar website trust. In fact, we found a significant, *negative* association between online activity and familiar website trust once we control for general trust and caution. This significant negative effect is sustained even when we control for level of knowledge of information technology and the experience of an adverse online event.

A likely explanation for the negative association of online activity with familiar website trust is that individuals who engage in more online activity also build a clear sense of prudence about their frequently visited websites. By definition, familiar websites are the ones individuals interact with on a regular basis. The more practical, first-hand experience individuals gain through online activities, the more they seem to believe that familiar websites are not particularly trustworthy—even though, ironically, they still use these sites. Frequent online activity allows individuals to become informed critics. Thus, individuals who engage in frequent online activity may build a broad sense of trust in websites in general, while simultaneously becoming more critical of the sites and services that they regularly use.

Our next group of hypotheses dealt with the relationships between an individual's broad tendencies toward trusting or not trusting others (general trust), being cautious of others or not (general caution), and the two forms of website trust. Overall, both general trust and general caution show strong positive relationships with general and familiar website trust. There is a clear link between general dispositions to trust others in interpersonal interactions and to trust interactions with web-based information systems. As the predicted probabilities in Table 4 reveal, individuals with the greatest levels of general trust and caution are associated with the highest amounts of general and familiar website trust. Just as in offline interactions, the most rewarding and prudent long-term strategy may be to couple high trust with high caution on the Internet (Cheshire et al. 2010).

We found one interesting exception regarding the association between general caution and general website trust: once we control for level of knowledge of information technology (model 3), general caution is no longer significantly associated with general website trust. Thus, it appears that one's own knowledge about information systems and the Internet is more critical to building general website trust than the underlying disposition to be cautious of others. We do not find the same drop in significance in the association between general caution and familiar website trust. This difference in results for the two types of trust demonstrates that competence tends to override broad dispositions to be cautious when one is assessing an equally broad type of interaction (websites in general on the Internet). However, when one is assessing familiar websites, the positive association between caution and web trust is a clear indicator of prudence and self-protection. In this case individuals who are more cautious may be insulating themselves by investing their trust in a restricted set of websites in response to a heightened sense of uncertainty and perceived risk.

Another key finding is the strong positive effect of level of knowledge of information technology on perceptions of general and familiar website trust. As the predicted probabilities in Table 4 illustrate, an individual who self-reports as highly competent with information technology is extremely likely to be in the upper categories (4–7) for both types of web trust, indicating high levels of trust. These probabilities are especially pronounced for familiar website trust: the cumulative probability of having very high familiar website trust (categories 5–7) is.92 for those with high IT knowledge. We expected this effect because higher self-reported knowledge of information technology (e.g., competence) should be an important part of reducing uncertainty. Those with high IT knowledge believe they have the capability to assess accurately the trustworthiness of the sites they use on a regular basis (familiar website trust) as well as websites more broadly (general website trust). Importantly, when we account for frequency of online behavior and dispositions to trust and be cautious of others, information technology competence remains a strong correlate of web trust.

We find that the experience of one or more adverse events online is significantly associated with a decrease in trust in websites in general, supporting our arguments about the experience of negative events and increased perceptions of uncertainty and risk on the Internet. One of the most surprising findings in our study is that the experience of an adverse online event is not related to one's level of familiar website trust. General website trust shows a clear, negative association with the experience of an adverse online event, but trust in familiar websites does not rise or fall simply because an individual has a bad incident on the Internet. One simple explanation is that adverse events may be less likely to occur in the context of familiar websites precisely because people might change their daily online websites after bad experiences occur. In this way, familiar websites are self-correcting because individuals may stop using systems that might be associated with an adverse event. Although familiar websites can become deeply embedded in daily habits, many people will remain sensitive to violations that occur in those contexts. Previous research has illustrated that individuals who are high in both general trust and general caution are particularly pro-active about managing their online risks and develop specific attitudes about risks and uncertainties in a given context (Cheshire

et al. 2010). Our findings do not suggest that one's trust attitudes about familiar websites are immune to the experience of adverse events, since we do not know when or where these events occurred for the respondent. However, it is reasonable to assume that individuals will choose to interact frequently with websites where the most risky adverse events are unlikely to occur. Furthermore, if the adverse event had nothing to do with a specific service (e.g., invasive spam email), then there is no reason to believe that an individual would draw a connection between familiar websites and the adverse event.

A second explanation for the lack of a relationship between adverse events and familiar website trust is related to the perception of a committed relationship between users and familiar, trusted websites. When people develop habits on the web they invest in a type of relationship with the websites that they frequently visit. Familiar websites become a part of life in the same way preferred organizations and companies do. When individuals develop a loyal relationship with websites and then experience an adverse event, it can create a contradictory relationship between perceptions known in social psychology as "cognitive dissonance". When an individual is faced with a salient contradiction between a belief and a relevant behavior, the individual will either escape the conflict entirely or change the belief or behavior to reduce the incongruity (Johnson et al. 1995). In the online context, the positive emotions and attitudes that result from website dependability can conflict with the negative consequences of a major adverse event such as a phishing attack or significant loss of data. If it is cumbersome or impractical to change daily habits by avoiding websites and online interactions altogether, many individuals may resolve the cognitive dissonance created by an adverse event by choosing to believe that the adverse event was not so bad after all or that it is unlikely to reoccur.

8 Implications and Future Directions

According to the Internet information company Alexa.com (2010), at least half of the top 12 websites in the world as of April 2010 are user-generated content and social networking sites (e.g., Facebook.com, Wikipedia.com, Twitter.com, Blogger.com), and the rest are primarily search engines and information portals (e.g., Google.com, Yahoo.com, Live.com). Only a decade ago the primary websites were major news websites, shopping sites and search engines. The Internet landscape is unquestionably shifting toward sites that aggregate and share content from *users* rather than from traditional, top–down news and information sources. However, the perpetually evolving capabilities and uses of websites raise important questions about best practices for online behavior and our ability to assess trust in complex online information systems.

Our results demonstrate that the experience of an adverse online event is negatively associated with general website trust, but curiously not with familiar website trust. We have previously argued that this may be due to changes in perception created by the reduction of the cognitive dissonance between attitudes and behavior, the modification to one's everyday websites in response to a negative incident, or a combination of both of these effects. However, our inability to detect an association between the experience of an adverse online event and familiar

website trust might also be explained by the non-specificity of our measure of adverse online events. Our measure captured all types of adverse online events as a single measure, meaning that we are unable to disentangle the effects of small problems (popup advertisements, spam email) versus larger and more destructive events (identity theft, privacy violations, scams).

Another issue with detecting adverse online events in familiar websites is that many threats to privacy and information control among the most popular websites have been invisible or difficult for users to notice. Some of the most high-profile infringements of privacy and norms of information sharing involve the largest and most popular online websites, including Facebook.com (Sullivan 2009; Walters 2009a, b) and Google.com (Helft 2010). For example, Facebook frequently changes its users' privacy settings and defaults, leading some to believe that most people must not understand the scope of what Facebook is collecting and sharing about them (Cashmore 2010). However, the popularity and visibility of Facebook has made it a target for lawmakers who are uncomfortable with Facebook's policy of automatically sharing users' personal information without their explicit consent (Guynn 2010). Although Facebook founder Mark Zuckerberg famously declared that "privacy is dead" (Walters 2009a), final judgment on this proclamation will depend on how users respond to the website as it evolves over time. As individuals become more informed about how social networking and user-generated content systems are using and sharing personal information and data, trust in these websites is likely to fluctuate. Detecting these changes in trust will require targeted measures of different adverse online events as they pertain to specific websites over time.

This research also has clear implications for research practitioners and designers who are interested in fostering and sustaining trustworthy online services and websites. Our results corroborate earlier findings (e.g., Gefen 2000) indicating that general trust is an essential factor in understanding what individuals actually do online. Our findings support the assertion that general website trust is a powerful and distinct attitude toward risk and uncertainty in web-based contexts. Indeed, additional insights might be gained by developing trust, reliability, credibility and security metrics for specific online systems. Importantly, our conception of general website trust focuses attention on the medium of the web as the context for general attitudes of confidence or caution. There are likely to be many distinctions to be made between trust attitudes in specific web-based domains such as online communication, financial transactions, and digital content production. With an increased attention to general trust, and a focus on specific profiles of risk and uncertainty, we can develop more complete and nuanced understandings of the links between different types or levels of trust and online behavior.

Finally, our findings also have implications for the production of website policies and the design of interfaces that are supportive of general and familiar website trust. Our results clearly show a strong association between IT knowledge and increased general and familiar website trust. An overarching implication of this research is that web-based systems should actively promote policies of information-sharing through clarity and simplicity wherever possible. Since self-reported information technology knowledge is strongly associated with web trust, one of the best ways to increase this knowledge is through transparency (a factor often linked to trust in other contexts). In our view a transparent web-based system is one which is open and communicative

about all aspects of the development, design, and operation of the system. In reality, many systems must be less than perfectly transparent about some features due to legal issues and concerns related to maintaining competitive advantage. However, maintaining information transparency is typically much better than creating virtual walls of undisclosed search algorithms and complex mechanisms for content ratings and rankings. By reducing uncertainty about their online system, website operators who make information transparency a design priority can empower their users and reap the benefits of greater perceived trustworthiness. These practices can lead to positive effects on the disposition of users to trust online systems and websites, potentially producing a long-run advantage for the larger Internet ecosystem.

Open Access This article is distributed under the terms of the Creative Commons Attribution Noncommercial License which permits any noncommercial use, distribution, and reproduction in any medium, provided the original author(s) and source are credited.

References

Alexa.com. (2010, April 16). Top 500 Global Sites. Retrieved from http://alexa.com/topsites

Baier, A. (1986). Trust and antitrust. *Ethics, 96*(2), 231–260.

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

Blau, P. M. (1964). *Exchange and power in social life*. New York: Wiley.

Cashmore, P. (2010, April 27). Nobody Can Stop Facebook Because Nobody Understands Facebook. Retrieved April 28, 2010, from http://mashable.com/2010/04/27/nobody-can-stop-facebook/

Chen, S. C., & Dhillon, G. S. (2003). Interpreting dimensions of consumer trust in e-commerce. *Information Technology and Management, 4*(2–3), 303–318.

Cheshire, C., Antin, J., & Churchill, E. (2010). Behaviors, Adverse Events, and Dispositions: An Empirical Study of Online Discretion and Information Control. *Journal of the American Society for Information Science and Technology, 61*(7), 1487–1501.

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

Cook, K. S. (2001). *Trust in Society*. Russell Sage Foundation Publications.

Cook, K. S., Cheshire, C., Gerbasi, A., & Aven, B. (2009a). Assessing trustworthiness in online goods and services. In K. S. Cook, C. Snijders, V. Buskens, & C. Cheshire (Eds.), *eTrust: forming relationships in the online world* (pp. 189–214). New York: Russell Sage.

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

Cook, K. S., Levi, M., & Hardin, R. (2009). *Whom Can We Trust?: How Groups, Networks, and Institutions Make Trust Possible*. New York: Sage.

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

Fogg, B. J., Jonathan, M., Tami, K., Joshua, S., Akshay, R., John, B., & Bonny, B. (2001). Web credibility research: a method for online experiments and early study results. CHI '01 extended abstracts on Human factors in computing systems.

Fogg, B. J., & Tseng, H. (1999). The elements of computer credibility. In *Proceedings of the SIGCHI conference on Human factors in computing systems: the CHI is the limit* (pp. 80–87). Pittsburgh, Pennsylvania, United States: ACM.

Friedman, B., Peter, H., Khan, J., & Howe, D. C. (2000). Trust online. *Communications of the ACM, 43* (12), 34–40.

Gefen, D. (2000). E-Commerce: the role of familiarity and trust. *Omega, 28*, 725–737.

Gefen, D., Karahanna, E., & Straub, D. W. (2003). Inexperience and experience with online stores: the importance of TAM and trust. *IEEE Transactions on Engineering Management, 50*(3), 307–321.

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.

Grabner-Krauter, S., & Kaluscha, E. (2003). Empirical research in on-line trust: a review and critical assessment. *International Journal of Human Computer Studies, 58*, 783–812.

Grabner-Krauter, S., Kaluscha, E. A., & Fladnitzer, M. (2006). Perspectives of online trust and similar constructs: a conceptual clarification. In *Proceedings of the 8th international conference on Electronic commerce: The new e-commerce: innovations for conquering current barriers, obstacles and limitations to conducting successful business on the internet* (pp. 235–243). Fredericton, New Brunswick, Canada: ACM.

Guynn, J. (2010, April 27). Four senators ask Facebook to make privacy fixes to new features. *The Los Angeles Times*. Retrieved April 28, 2010, from http://www.latimes.com/business/la-fi-facebook-20100427-1,0,4386095.story

Hardin, R. (2001). Conceptions and Explanations of Trust. In K. S. Cook (Ed.), *Trust in Society* (pp. 3–39). Russell Sage Foundation Publications.

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

Harris, L., & Goode, M. (2004). The four levels of loyalty and the pivotal role of trust: a study of online service dynamics. *Journal of Retailing, 80*(1), 139–158.

Hayashi, C., Suzuki, T., Suzuki, G., & Murakami, M. (1982). *A study of Japanese National character*. Tokyo: Idemitsushoten.

Helft, M. (2010, February 15). Anger leads to apology from Google about Buzz. *The New York Times*. Retrieved 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.

Horrigan, J. B. (2007). *A typology of information and communication technology users*. Washington: Pew Internet & American Life Project.

Johnson, R. W., Kelly, R. J., & LeBlanc, B. A. (1995). Motivational basis of dissonance: aversive consequences or inconsistency. *Personality and Social Psychology Bulletin, 21*(8), 850–855.

Kollock, P. (1999). The Production of Trust in Online Markets. In *Advances in Group Processes*. Greenwich, CT: JAI Press.

Luhmann, N. (1979). *Trust and power*. Chichester: Wiley.

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

Marsh, S., & Dibben, M. R. (2003). The role of trust in information science and technology. *Annual Review of Information Science and Technology, 37*, 465–498.

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

Nass, C. I., Steuer, J., & Tauber, E. R. (1994). Computers are social actors. Proceedings of the SIGCHI conference on Human factors in computing systems: celebrating interdependence.

Nissenbaum, H. (2001). Securing trust online: wisdom or oxymoron. *Boston University Law Review, 81*, 635.

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.

Olson, G. M., & Olson, J. S. (2000a). Distance matters. *Human-Computer Interaction, 15*(1), 139–178.

Olson, J., & Olson, G. M. (2000b). i2i Trust in E-Commerce. *Communications of the ACM*, *43*(12), 41–44.

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

Riegelsberger, J., Sasse, M. A., & McCarthy, J. D. (2003). The researcher's dilemma: evaluating trust in computer-mediated communication. *International Journal of Human Computer Studies, 58*(6), 759–781.

Rotter, J. (1967). A new scale for the measurement of interpersonal trust. *Journal of Personality, 35*(1), 651–665.

Suh, B., & Han, I. (2002). Effect of trust on customer acceptance of Internet banking. *Electronic Commerce Research and Applications, 1*(3), 247–263.

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

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

Yamagishi, T. (1998). *The structure of trust: the evolutionary game of mind and society.* Tokyo: University of Tokyo Press.

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.

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.

Yoon, S. (2002). The antecedents and consequences of trust in online-purchase decisions. *Journal of Interactive Marketing, 16*(2), 47–63.