2 Privacy, trust, and disclosure online

Carina B. Paine and Adam N. Joinson

Introduction

The use of new technology, and particularly the Internet, increasingly requires people to disclose personal information online for various reasons. In computer-mediated communication, disclosure may serve to reduce uncertainty in an interaction (Tidwell & Walther, 2002) or to establish legitimacy when joining an online group (Galegher, Sproull, & Kiesler, 1998). Disclosure is often a prerequisite to access services (for instance, with the ubiquitous registration form), to make online purchases (Metzger, 2006) or is requested for those same services to be personalized. The increasingly social nature of much web-based software (e.g., social network sites) also places a privacy cost on users due to a heightened requirement for disclosure of personal information as part of the functionality of the system (see Glaser, 2006). In addition to this increased need for disclosure, the development of ambient and ubiquitous technologies has raised the possibility that devices will communicate, or even broadcast, personal information without recourse to the user. Moreover, the ability to store information easily and cross-reference databases raises the possibility of unwitting disclosure through information accrual. Perhaps not surprisingly, this has raised a number of privacy concerns, among consumers and privacy advocates (e.g., Jupiter Research, 2002; U.K. Information Commissioner, 2006).

We start this chapter by introducing the existing research literature surrounding privacy and trust online. We then go on to consider how privacy and trust interact in determining online behavior. Finally, the chapter concludes with the description of a number of steps that can be taken to ensure that social software both protects privacy and enables the development of trust.

Privacy

What is privacy?

There have been several attempts to define privacy. In a legal context, privacy has been considered to be largely synonymous with a “right to be let alone” (Warren & Brandeis, 1890). Within psychological literature both Westin’s and

P1: IBE
9780521873017c02 CUFX259/Barak 978 0 521 87301 7 November 14, 2007 12:1

Altman's theories figure prominently in the major reviews of privacy in the 1970s. Westin (1967) provides a link between secrecy and privacy and defines privacy as "the claim of individuals, groups, or institutions to determine for themselves when, how and to what extent information about them is communicated to others" (p. 7). Altman (1975) incorporates both social and environmental psychology in understanding the nature of privacy. He defines privacy as "the selective control of access to the self" (p. 24) and believes privacy is achieved through the regulation of social interaction, which can in turn provide us with feedback on our ability to deal with the world and ultimately affect our definition of self. Both Westin's and Altman's theories have stimulated much of the research and theory development of privacy. However, despite many attempts to create a synthesis of the existing literature in this area (e.g., Parent, 1983; Schoeman, 1984), a unified and simple account of privacy has yet to emerge.

Dimensions of privacy

The highly complex nature of privacy has resulted in an alternative way of defining it, through its various dimensions. Burgoon et al. (1989) and DeCew (1997) have both developed multidimensional definitions of privacy. Burgoon et al. (1989) distinguish four dimensions of privacy and define it using these dimensions as "the ability to control and limit *physical*, *interactional*, *psychological* and *informational* access to the self or one's group" (p. 132). DeCew (1997) also reflects the multidimensional nature of privacy in her definition, which distinguishes three dimensions: *informational*, *accessibility*, and *expressive privacy*. There is much overlap between these multidimensional approaches, and some overlap between the features of each dimension. The broad features for each of the main dimensions are described below:

- *Informational (psychological) privacy* – relates to an individual's right to determine how, when, and to what extent information about the self will be released to another person (Westin, 1967) or to an organization. It covers personal information such as finances, medical details, and so on that an individual can decide who has access to and for what purposes.
- *Accessibility (physical) privacy* – relates to the degree to which a person is physically accessible to others. It "allows individuals to control decisions about who has physical access to their persons through sense perception, observation, or bodily contact" (DeCew, 1997, pp. 76–77). This dimension is grounded within our biological need for personal space.
- *Expressive (interactional) privacy* – "protects a realm for expressing ones self-identity or personhood through speech or activity. It protects the ability to decide to continue or to modify ones behaviour when

the activity in question helps define oneself as a person, shielded from interference, pressure and coercion from government or from other individuals" (DeCew, 1997, p. 77). As such, internal control over self expression and the ability to build interpersonal relationships improves, while external social control over lifestyle choices and so on are restricted (Schoeman, 1992).

Actual privacy and perceived privacy

Finally, a distinction can also be made between *actual* privacy and *perceived* privacy. These two forms of privacy coexist, and there will often be a mismatch between the two. For example, a person's perceived privacy may be high when they have control over disclosing their personal information to an online store. However, their actual privacy may be low due to the unobtrusive (automatic) collection of their online behavior, and the potential future use of the information they provide by unknown third parties.

More obtrusive invasions of privacy may result in a reduction of perceived privacy alongside actual privacy. For example, in the television program *Big Brother*, a number of housemates live together for several weeks, surrounded by hidden television cameras and microphones. Although housemates may enter the Big Brother house with low levels of perceived privacy (and low levels of actual privacy), over time their perceived privacy will increase (as the cameras are forgotten about), but their actual privacy will remain low.

The importance of privacy

Despite there being no unitary concept of privacy, it is clear that both individuals, and society, attach a level of importance to it. For example, Ingham (1978) states that "man, we are repeatedly told is a social animal, and yet he constantly seeks to achieve a state of privacy" (p. 45). A failure to achieve any level of privacy will result in "costs." For example, by not obtaining privacy, a person will not benefit from the opportunities that the functions of privacy provide, which could result in stress or negative feedback about the self. There are also costs of losing privacy either through privacy invasion (when conditions for privacy are not achieved e.g., being overheard) or privacy violation (when recipients of personal information – intentionally provided by the discloser or gained through a privacy invasion – pass it on to others, e.g., gossip).

In the early privacy research described, invasions and violations were not emphasized. If they were, they were not considered to be an issue for daily life. For example, Ingham (1978) also states, "In everyday social life most individuals are only rarely confronted with an invasion of their privacy, although the number of potential threats is very large" (p. 40). However, since this early

P1: IBE
9780521873017c02 CUFX259/Barak 978 0 521 87301 7 November 14, 2007 12:1

research, new technology (and in particular the Internet) has fueled debate and controversy about potential invasions and violations to privacy (Dinev & Hart, 2004) as will be described below.

Privacy and the Internet

> At no time have privacy issues taken on greater significance than in recent years, as technological developments have led to the emergence of an "information society" capable of gathering, storing and disseminating increasing amounts of data about individuals. (Schatz Byford, 1996, p. 1)

Over recent years, the Internet has become an important and ubiquitous feature of daily life in the developed world (e.g., online shopping, the sharing of documents, and various forms of online communication). With this increased use of the Internet, the way information is gathered and used has changed. A wide variety of information data is now collected with increasing frequency and in different contexts, making individuals become ever more transparent. The costs of obtaining and analyzing this data are also decreasing with the advances in technology. As recognition of this phenomenon grows, the issue of privacy has increased in salience. There are concerns that the Internet seems to erode privacy (Rust, Kannan, & Peng, 2002) and that offline privacy concerns are magnified online (Privacy Knowledge Base, 2005).

There are a number of specific threats to privacy online. For example, the effect of "ubiquitous" computing (Weiser, 1988) means that we leave data footprints in many areas of our lives that were previously considered "offline." The extremely rapid development of computing power, in terms of greater processing speed, increased storage capacity, wider communication connectivity, and lower machine size all affect privacy (Sparck-Jones, 2003). Specifically, the Internet's feature of *connectivity* (Sparck-Jones, 2003) means that it allows for interactive two-way communication and is woven into people's lives in a more intimate way than some other media as it connects people with places and people with people. Accordingly, it poses unique information privacy threats. These rapid advances mean that information can be efficiently and cheaply collected, stored, and exchanged, even data that may be deemed sensitive by the individuals concerned. As such, massive databases and Internet records of information about individual financial and credit history, medical records, purchases, and so on exist.

Therefore, there are important privacy issues related to online activities (Earp, Anton, Aiman-Smith, & Stufflebeam, 2005) as mundane as buying your weekly groceries over the web (e.g., does the retailer store information on your purchases? Is it sold to third parties so they can send you targeted junk mail?) or as specialized as online psychological research (e.g., is identifying information gathered about participants? Can confidentiality be guaranteed?).

P1: IBE
9780521873017c02 CUFX259/Barak 978 0 521 87301 7 November 14, 2007 12:1

Of course, there are also *benefits* to the technological advances described (personalized service, convenience, improved efficiency). Users can trade off providing valuable information about themselves to take advantage of such benefits. The Pew Internet and American Life Survey (2001) reported that over two-thirds of users are willing to share their personal information under some circumstances. In some situations, expressive privacy may be obtained through the loss of informational privacy to a third party. For example, one may disclose personal details and credit card information to have the convenience of completing an online transaction. In this way, the collection of personal, privacy information can be considered a “double-edged sword” (Malhotra, Kim, & Agarwal, 2004).

Measuring privacy

Privacy can be both objective (actual privacy) and subjective (perceived privacy). It is also a dispositional preference (Larson & Chastain, 1990) and a situational characteristic (Margulis, 2003). So, while people might be more or less concerned with their privacy *in general*, situational factors such as the costs and benefits of protecting or revealing information (Acquisti, 2004) combine to determine whether information is disclosed. To complicate matters further, privacy is also dynamic in that it serves to regulate social interaction (Altman, 1975; Derlega & Chaikin, 1977), while at the same time it can highlight uneven power relations (Derlega & Chaikin, 1977) or signify trust (Altman, 1977). Naturally, the complicated nature of privacy poses measurement issues. Generally, the measurement of privacy in online environments focuses on people’s privacy concerns (i.e., their subjective attitudes about privacy) or their perceived privacy within a specific interaction.

Several studies have attempted to measure privacy concerns in detail and to identify different types of privacy concern. However, such studies tend to focus on informational privacy, and privacy scales are usually approached with a view of privacy as a one-dimensional construct. The Concern for Information Privacy (CFIP) scale was developed by Smith, Milberg, and Burke (1996). It was the first measure of its kind and measured individuals’ concern regarding organizational practices. Later research (e.g., Stewart & Segars, 2002) argued that the CFIP needed to be reevaluated and developed following advances in technology, research, and practice. More recently, Malhotra et al. (2004) operationalized a more multidimensional notion of Internet Users Information Privacy Concerns. Their model (and measuring instrument) recognizes that there are multiple aspects of privacy. However, all of these aspects still lie within the domain of informational privacy, and other dimensions are not addressed.

Harper and Singleton (2001) suggest that one of the main defects of most privacy surveys and studies is that they do not separate out all of the different factors that could be considered privacy issues. It is clear from the definitions of privacy that it is a multifaceted concept, and therefore that scales attempting to measure concern should tap these different facets about which people may be concerned. For instance, Paine, Reips, Stieger, Joinson, and Buchanan (2007) used an automated interview agent to collect Internet users' privacy concerns and report a wide variety of noninformation types of privacy concerns, including viruses and spam.

In addition, following interviews with and observations of Internet users, Viseu, Clement, and Aspinall (2004), suggest that the privacy discourse should be reevaluated to comprise all of the moments involved in online use (the moment of sitting in front of a computer; the moment of interacting with it; and the moment after information has been released).

Furthermore, as well as attitudes and concerns about privacy, it is important to consider behaviors people may adopt to safeguard their privacy. There is a complex relationship between attitude and behavior in this context. For example, a computer virus can be seen as an invasion of privacy. We may be concerned about the possibility of a virus and take steps to prevent it (use of an antivirus software or an operating system less vulnerable to viruses). Concern prompts us to take preventative measures, but knowing that measures have been taken could reduce our level of concern (Paine et al. [2007] found that some people reported that they were not concerned about privacy, and when asked why stated that they had taken action to protect their privacy). Therefore, privacy measurements need to measure privacy concerns and privacy-related behaviors to produce a complete picture. Buchanan, Paine, Joinson, and Reips (2007) have recently developed a measure of online privacy concern that covers different dimensions of privacy, as well as including protective behavioral items.

Trust

What is trust?

Bargh and McKenna (2004) describe using the Internet as a "leap of faith." If we contact a potential partner via an online dating site, there is no way of knowing whether they are as they have described themselves in their profile or subsequent communication. When we work in virtual teams, or join virtual communities, we take it on faith that the people we talk to are whom they say. Purchasing online compared with from a bricks-and-mortar store requires a belief that the goods will arrive, that they will be as described on the website, and that your credit card and personal information will not be traded or otherwise misused And, when we seek advice online, we often do not know who the authors of the advice are, and what motivates them to help us.

In these kinds of scenarios, trust is critical in determining people's behavior. Trust has been studied in many different disciplines, and there are a large number of potential definitions (Corritore, Kracher, & Wiedenbeck, 2003; Green, 2007). There is broad agreement, however, that trust is critical when there is a degree of uncertainty (Mayer, Davis, & Schoorman, 1995). This uncertainty also needs to contain an element of risk (Deutsch, 1962). Without any risk, or vulnerability, there is no need for trust (Mayer et al., 1995).

Trust is the "willingness to be vulnerable, based on positive expectations about the actions of others" (Bos, Olson, Gergle, Olson, & Wright, 2002, p. 1). In an interpersonal context, it can be defined as holding "confident expectations of positive outcomes from an intimate partner" (Holmes & Rempel, 1989, p. 188) or "an expectancy held by individuals or groups that the word, promise, verbal, or written statement of another can be relied on" (Rotter, 1967, p. 651). Trust can be a personality trait or disposition, with some people more trusting that others (Mayer et al., 1995). It is also an attitude or belief about the intentions of a specific other (McKnight, Cummings, & Chervany, 1998). It can be generalized (you trust a person or group across all domains) or specific to an interaction (you trust a person only in one domain). There is general agreement that trust is best conceptualized as multidimensional (Bhattacherjee, 2002; Gefen, 2002; Mayer et al., 1995). That is, trust comprises a number of unique aspects that, although interrelated, are also discernable. Bhattacherjee (2002) identifies three main dimensions of trust: ability, integrity, and benevolence.

- *Ability* – refers to the knowledge, skills, and competence of the person trusted to conduct the expected actions. In an e-commerce (electronic commerce) setting, this might be the expectation that an online store has the ability to take an order and process it and will do so without accidentally revealing personal information. According to Bhattacherjee (2002), this dimension of trust is domain specific, that is, trust in one area (e.g., to provide the book we ordered) does not transfer to other domains (e.g., we would not necessarily trust Amazon to provide us with health advice).
- *Integrity* – refers to the belief that the person or institution will act in an honest, reliable, and credible manner (Jarvenpaa, Knoll, & Leidner, 1998). That is, they will adhere to the usual rules or expectations that are perceived as fair to both parties and will not violate the trust placed in them (i.e., you have confidence in the person or organization you are trusting). In an interpersonal context, integrity would reflect your confidence that the person you are trusting will not violate that trust, and it has a strong element of predictability (i.e., you have confidence in how the other person will behave in the future). In e-commerce, integrity would refer to a belief that the organization you are dealing with is honest, reliable, and will keep its promises (Gefen, 2002).
- *Benevolence* – refers to "the extent to which a trustee is believed to intend doing good to the trustor" (Bhattacherjee, 2002, p. 219). In a commercial setting, this might be reflected in beliefs that a company

has its customers' best interests at heart (although this does not rule out making a legitimate profit). Benevolent organizations do not make excessive profits or exploit their customers. In an interpersonal setting, benevolence would refer to the belief that the person giving you advice is doing so to help you, not himself/herself (or a third party).

Trust and the internet

On the Internet, we often take a leap of faith that the people or organizations we deal with can be trusted. Moreover, lack of trust is a problem for online organizations: "If the web site does not lead the consumer to believe that the merchant is trustworthy, no purchase decision will result" (Ang & Lee, 2000, p. 3). Trust is also essential for cooperation (Deutsch, 1962) and for effective teamwork (whether face-to-face or mediated; Bos et al., 2002). Trust is also critical in understanding when we choose to share with others and when we choose secrecy (Altman, 1977).

Is trust reduced online?

Handy (1995) states that "trust needs touch." This reflects the widely held belief that trust between people is poorly established in lean, mediated environments (e.g., Tanis & Postmes, 2007). To examine whether trust does need touch, Bos et al. (2002) compared trust ratings and cooperation between team members across four different conditions: face-to-face, audio conferencing, videoconferencing, and text chat. The three-person teams were playing a trust game in which cooperation maximized the potential gains for all members, while a competitive strategy reduced the likelihood of a higher gain. Bos et al. predicted that trust would be lowest and performance impeded in the lean media condition. Their results confirmed their predictions: The text chat groups scored the experience lowest in trust and gained the lowest amount of points in the game (signifying a competitive strategy). However, the Bos et al. study may not be strong evidence for trust needing touch. First, the experimenters banned social conversation from the experiment. This immediately placed the "richer" media conditions at an advantage because visual and aural cues normally compensated for in CMC (computer-mediated communication) social communication could not be in this sterile environment. Second, and related, such games are artificial in the extreme and have little relationship to how people actually use media. Third, the time given to the experiment was not sufficient for the text-based condition to "catch up" with the media with faster communication exchange (Walther, 1992). Finally, the use of self-reports for trust is unreliable because people tend to rate richer media as higher in trust, despite evidence that communication is more effective without identity cues for experienced users (Tanis & Postmes, 2007).

Building trust online

There are a number of techniques that people engage in to build trust in interpersonal computer-mediated communication. Researchers have found that on the Internet individuals go about reducing uncertainty by asking more direct, probing questions (Tidwell & Walther, 2002). If this is responded to with heightened self-disclosure (Joinson, 2001a), and reciprocated (Joinson, 2001b), then a cycle of hyperpersonal interaction might occur (Walther, 1996). The use of profiles, and particularly photographs, is also designed to increase the level of trust at an interpersonal level (Tanis & Postmes, 2007; Whitty & Carr, 2006). A further method for increasing trust in interpersonal interaction is media switching. Internet relationships tend to follow a similar pattern of initial contact in a public arena, then to a private domain (e.g., email or AOL messenger), then to the telephone, and then to face-to-face meetings (McKenna, Green, & Gleason, 2002; Parks & Floyd, 1996; Whitty & Gavin, 2001). This movement is not only a signifier of trust (I trust you enough to give you my phone number), but it is also a way that identities can be established, and the *faith* shown earlier on rewarded with *predictability* and, perhaps, *dependability*.

People also use linguistic cues to convey trustworthiness. Galegher et al. (1998) examined the messages of three Usenet support groups and three hobby groups collected for a three-week period to look for clues about how their members established legitimacy and credibility. The group members created legitimacy in a number of ways. They posted messages appropriate to the group, and use snappy headers to make themselves "heard." Galegher et al. note that often posters refer to their own membership of the electronic group, or how long they have lurked for before asking a question/replying to one. Even frequent posters included references to their members of the group 80 percent of the time when asking questions. Posters often signal their membership of the specific problem group (e.g., depression) by introducing information on their diagnosis, prescription, or symptoms. In the support groups Galegher et al. studied, 80 questions received no reply. Most lacked any legitimizing information of the type outlined previously and were generally simply requests for information rather like complex database queries. In the hobby groups, evidence of such legitimacy seeking was much less apparent.

Within pseudonymous environments, reputation systems also provide an important marker for a person's trustworthiness (Resnick, Kuwabara, Zeckhauser, & Friedman, 2000). The most well-known reputation system is that used by eBay. In the eBay system, users leave positive, neutral, or negative feedback, plus a short comment, for each transaction. Resnick and Zeckhauser (2001) studied the eBay reputation system and reported that the feedback given did seem to predict the sellers' future success, including the chances that their goods would be bought.

With the rise of social computing of "Web 2.0" sites, reputation systems have spread, such that it is now common to find community systems with rankings for members based on (among others) longevity, number of postings, and (for the highest ranks) a form of peer review. The ability to "Digg" or "Bury" stories acts as a form of community-derived trust building. Many of the "blog commenting systems also now incorporate systems for reader rating of comments, and the hiding of poorly ranked comments.

Many e-commerce sites include privacy policies that contain descriptions of their privacy practices for the online collection, use, and dissemination of personal information. Many of these policies address privacy issues in all contexts (i.e., both the primary and secondary use of data). Another development has been the use of web-based seals, for example TRUSTe (see http://www.truste.org/) and Trust UK (see http://www.trustuk.org.uk/). These seals are a visible way to assure customers that online businesses respect an individual's privacy on the Internet and are designed to enable consumers to "buy online with confidence" (Trust UK).

However, there has been mixed research on the use of privacy polices and web-based seals. Liu, Marchewka, Lu, and Yu (2005) found that that levels of trust can be increased by integrating a comprehensive privacy policy into the design of an e-commerce website and that having a privacy policy may lead to a customer returning to a site and making further purchases. However, much research (e.g., Tsai, Cranor, Acquisti, & Fong, 2006) has found that although the majority of users tend to notice the presence of privacy policies, they rarely read them. In addition, using a mock commercial website, Metzger (2006) found that it is the reputation of a company that is important in influencing trust and disclosure of personal information online, not privacy assurances. This finding suggests that despite efforts of online companies to communicate trustworthiness through their strong privacy policies, it is a company's reputation that promotes trust and subsequently disclosure.

Other research has suggested a more far-reaching approach to reducing privacy concerns and gaining trust online in e-commerce. For example, Viseu et al. (2004) suggest websites display their compliance with "fair information practices" prominently (e.g., at the point where users are required to enter their personal information) rather than in "hard to find" and incomprehensible privacy statements. Another approach is suggested by Boyd (2003) who hypothesizes that trust online is built through rhetorical devices such as providing descriptions of websites credentials and competencies, display customer feedback, records of past security performance, and offering simple and clear assessments of risk to potential customers.

Measuring trust

Like privacy, trust can be measured at many different levels (Corritore et al., 2003). It can be treated as a disposition or personality trait, or as a specific state associated with a single interaction episode. Most studies of trust online have tended to focus on the latter, more specific aspect of trust. As we also noted,

Table 2.1. *Trust items and factor loading*

Item	Loading
I felt comfortable giving my personal information	.43
The data I have provided will be kept secure and not exploited	.70
The intentions of this survey are good	.84
I do not doubt the honesty of this survey or its authors	.81
This survey's authors are a dependable research group	.90
This survey's authors have the appropriate skills and competence to conduct online surveys	.89
This survey is professional	.86
The authors of the survey are trustworthy	.89

trust is multidimensional, with each dimension associated with the nature of the specific interaction. For instance, the competence of an online retailer might be related to their ability to deliver a product or service as desired. However, when you trust someone with your secrets, competence might mean believing that they will not accidentally forward your e-mail to the whole department (or print it and forget to collect).

Measures of trust tend to be specific to individual studies, then. For instance, Jarvenpaa, Tractinsky, and Vitale (2000) used seven items to assess trust, ranging from "This store is trustworthy" to, "This store wants to be known as one who keeps promises and commitments," and, "I trust this store keeps my best interests in mind." Gefen (2002) developed a similar scale, based on the three dimensions of integrity, benevolence, and ability. His nine-item scale includes items such as, "Promises made by Amazon.com are likely to be reliable" (Integrity), "I expect that Amazon.com are well meaning" (Benevolence), and "Amazon.com knows how to provide excellent service" (Competence).

Measures of interpersonal trust in CMC research have also tended to use a multidimensional approach. Bos et al. (2002) used an eleven-item scale consisting of items such as, "The other players in the game could be trusted," and "The other players always told me the truth" to measure trust in (competitive) virtual teams. They also used overall payouts as a behavioral measure of trust, on the assumption that high trust would lead to greater cooperation and higher payouts in the game. But, Riegelsberger, Sasse, and McCarthy (2003) question the utility of these kinds of "prisoner's dilemma" games for measuring trust in CMC and recommend it only for specific situations.

In our own research (e.g., Paine, Joinson, Buchanan, & Reips, 2006), we have developed a measure of trust for use in online research that reflects the three different dimensions. Specifically, the measure reflects trust in the competence, benevolence, and integrity of a researcher, enabling us to host materials online easily and assess their trustworthiness. These items are outlined below, in Table 2.1, alongside their factor loadings using principal components

P1: IBE
9780521873017c02 CUFX259/Barak 978 0 521 87301 7 November 14, 2007 12:1

analysis yielding a single factor (without rotation) that explains 65 percent of the variance ($n = 690$). Forcing a two-factor solution yielded a single-item second factor based on the first item. For this reason, it is suggested that all items, except the first ("I felt comfortable giving my personal information"), are used as a single scale to measure trust. In this format, the scale has an internal reliability (Cronbach's alpha) of .93.

Privacy, trust, and online behaviour

Although we have discussed privacy and trust as separate dimensions, there is considerable evidence that they interact in determining online behavior. Online privacy is often framed as a contributor to trust, rather than as an independent effect on online behavior. For instance, the Google, Inc., privacy counsel for Europe justified the anonymizing of search data by saying, "We believe that privacy is one of the cornerstones of trust" (The Guardian, March 15, 2007). It has also been repeatedly reported that trust is a significant precursor to the disclosure of information online (e.g., Heijden & Verhagen, 2002; Hoffman, Novak, & Peralta, 1999; Jarvenpaa and Tractinsky, 1999; Jarvenpaa et al., 2000; Metzger, 2004). Specifically, Jarvenpaa and Tractinsky (1999) found that trust increases confidence in a company and therefore increases the likelihood of consumers engaging in transactions online. This relationship is borne out in a series of research findings. For instance, Malhotra et al. (2004) examined the links between people's Internet information privacy concerns and their related behavioral intentions. They found that the effect of privacy concerns on behavioral intentions was mediated by trust. Similarly, Chellappa and Sin (2005) studied consumer's intent to use personalization services. They also found that this intent was influenced by both trust and concern for privacy. Metzger (2004) asked participants to evaluate a fictitious commercial website and found that the effect of participants' general concern for privacy and the degree to which they believed e-commerce websites protect their privacy on disclosure was mediated by trust.

In the traditional sense, mediation refers to the effect of an independent variable on a dependent variable being explained by common links to a third variable (i.e., the mediator; Baron & Kenny, 1986). The reported results would therefore suggest that privacy has no direct effect on behavior; instead, any effect could be explained by the links between privacy and trust and between trust and behavior.

Indeed, although many Internet users express privacy-protectionist attitudes, this rarely translates to their actual behavior (Metzger, 2006; Pew Internet and American Life Project, 2000). For instance, Spiekermann, Grossklags, and Berendt (2001) measured the privacy preferences of 171 users and observed their behavior on a mock e-commerce site. On this site, the users were "helped" by a ‘bot (short for an automated agent or “robot”) that asked a number of purchase-related questions of differing levels of intrusiveness. They found very little evidence that privacy preferences were related to people’s actual behavior in response to the ‘bot’s questions. Similarly, Metzger (2006) found no association between people’s privacy concerns and their disclosure to an e-commerce site nor between the content of a privacy policy or presence of a privacy seal and disclosure behavior. The failure of various privacy-enhancing technologies in the marketplace also suggests a disjunction between people’s stated attitudes and their actual actions to protect their privacy (Acquisti & Grossklags, 2003).

Liu et al. (2005) propose a “privacy-trust-behavioural intention” model in e-commerce. In their study, they manipulated participants’ levels of privacy in fictional websites (by either including a privacy policy or not). They found that privacy has a strong influence on whether someone trusts an e-commerce business. In turn, this level of trust will influence their behavioral intention to purchase from a site.

Recently, our own work has considered whether privacy and trust operate in a mediation or moderator relationship (Joinson, Paine, Buchanan, & Reips, under review). In a series of longitudinal and experimental studies, we found evidence that the effect of perceived privacy on disclosure was mediated by trust at a situational level but also evidence for moderation when privacy and trust were experimentally manipulated. That is, we found evidence that trust and privacy interact to determine disclosure behavior, such that high privacy compensates for low trustworthiness, and high trustworthiness compensates for low privacy. Clearly, privacy and trust are closely related in predicting people’s willingness to disclose personal information, and the relationship may be more nuanced than simple mediation.

Summary and conclusions

As we have seen earlier in this chapter, issues of privacy and trust are critical not only for the design of computer systems but also in how research is conducted online. We believe that the protection of privacy (in its various forms), alongside mechanisms to promote trust, are critical to both the design of social systems online as well as being important considerations for people aiming to conduct research using the Internet.

However, the rapid development of the e-society poses unique challenges for privacy due to the increased requirement for self-disclosure on an interpersonal and person-organization level. Similarly, using the Internet to collect survey data poses privacy challenges for researchers that can unduly influence response patterns (Joinson, Woodley, & Reips, 2007). There are a number of steps that can be taken to ensure that social software both protects privacy and enables the development of trust.

First, system developers should implement guidelines to limit the amount of personal information collected and privacy policies that require disclosure on a "need-to-know" basis rather than a general assumption that all administrators have full access to users' data. Where possible, identity management solutions should be implemented, even if only at the level of the user interface. For instance, a simple identity management system would be the implementation of pseudonyms within educational virtual learning environments. At the moment, the default option is often to link a publicly accessible learning resource (e.g., a blog or asynchronous conference) directly to the students' real identity. This poses not only an issue as far as informational privacy is concerned but may also limit expressive privacy. By building a simple identity management system that links a pseudonym to the users' real identity, but does not make that link publicly accessible, it is possible to encourage expressive privacy, and with it more effective educational outcomes. Other system design features can be used to protect privacy – for instance, implementing distributed systems rather than centralized data stores tends to be both more secure and less prone to data mining. This can be seen in Internet use too: People who use the same pseudonym across many Internet environments are more easily tracked than those who use various pseudonyms.

Second, trust needs to be built into the design of Internet services, either through the enabling of trust-building activities or the use of trust cues and mechanisms. So, in the case of computer-supported collaborative work, we have seen that trust can be encouraged by allowing users time to exchange socio-emotional messages, rather than forcing them to focus only on task-based communication. Reputation systems also provide a mechanism to develop trust (and to shortcut some of the time taken to build a trusting relationship).

Third, where possible, users should be provided with control over whether to disclose personal information and the use of that personal information once disclosed. In our own research, we have found that the provision of a simple "I prefer not to say" option to sensitive questions in surveys is an effective method for the protection of privacy (Joinson & Reips, 2007) by providing control over whether to disclose. In cases where there is an imperative to collect some information, control can take the form of providing ways for people to disclose information with relatively low diagnosticity. For instance, ambiguity is a well-established mechanism for disclosing information with low information value – if one is asked about a current location, it is possible to "blur" the response by being vague (e.g., "I am in Milton Keynes") rather than precise (e.g., "I am in my office").

We believe that the implementation of these principles to the design of online environments will not only protect privacy for ethical purposes but will also enable much of the rich interaction many people seek when online. The excessive collection of personal information, and loss of trust, poses a challenge to beneficial use of the Internet and threatens to create a surveillance culture lacking in rich social interaction or diverse content. As social scientists, we must promote the development of a socially responsible cyberspace that is of benefit to all its citizens.

Acknowledgments

The writing of this chapter was supported by funding from the U.K. Economic and Social Research Council E-Society Programme (RES-341-25-0011). We are grateful to Azy Barak and Alexander Voiskownsky for their insightful comments on an earlier draft.

References

Acquisti, A. (2004). Privacy in electronic commerce and the economics of immediate gratification. In *Proceedings of the ACM Electronic Commerce Conference* (EC 04; pp. 21–29). New York, NY: ACM Press.

Acquisti, A., & Grossklags, J. (2003). *Losses, gains, and hyperbolic discounting: An experimental approach to information security attitudes and behavior*. Second Annual Workshop on "Economics and Information Security."

Altman, I. (1975). *The environment and social behaviour*. Monterey, CA: Brooks/Cole.

Altman, I. (1977). Privacy regulation: Culturally universal or culturally specific? *Journal of Social Issues, 33*, 66–84.

Ang, L., & Lee, B.-C. (2000). Influencing perceptions of trustworthiness in Internet commerce: A rational choice framework. In *Proceedings of Fifth CollECTer Conference on Electronic Commerce* (pp. 1–12). Brisbane.

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

Bhattacherjee, A. (2002). Individual trust in online firms: Scale development and initial test. *Journal of Management Information Systems, 19*, 211–241.

Bos, N., Olson, J. S., Gergle, D., Olson, G. M., & Wright, Z. (2002). Rich media helps trust development. In *Proceedings of CHI 2002* (pp. 135–140). New York: ACM Press.

Boyd, J. (2003). The rhetorical construction of trust online. *Communication Theory, 13*, 392–410.

Buchanan, T., Paine, C. B., Joinson, A. N., & Reips, U.-D. (2007). Development of measures of online privacy concern and protection for use on the Internet. *Journal of the American Society for Information Science and Technology, 58*, 157–165.

Burgoon, J. K., Parrott, R., LePoire, B. A., Kelley, D. L., Walther, J. B., & Perry, D. (1989). Maintaining and restoring privacy through communication in different types of relationship. *Journal of Social and Personal Relationships, 6*, 131–158.

Chellappa, R. K., & Sin, R. G. (2005). Personalization versus privacy: An empirical examination of the online consumer's dilemma. *Information Technology and Management, 6*, 181–202.

Corritore, C. L., Kracher, B., & Wiedenbeck, S. (2003). On-line trust: Concepts, evolving themes, a model. *International Journal of Human-Computer Studies, 58*, 737–758.

DeCew, J. (1997). *In pursuit of privacy: Law, ethics, and the rise of technology*. Ithaca, NY: Cornell University Press.

Derlega, V. J., & Chaikin, A. L. (1977). Privacy and self-disclosure in social relationships. *Journal of Social Issues, 33*, 102–115.

Deutsch, M. (1962). Cooperation and trust: Some theoretical notes. *Nebraska Symposium on Motivation, 10*, 275–318.

Dinev, T., & Hart, P. (2004). Internet privacy concerns and their antecedents – Measurement validity and a regression model. *Behaviour and Information Technology, 23*, 413–423.

Earp, J. B., Anton, A. I., Aiman-Smith, L., & Stufflebeam, W. H. (2005). Examining Internet privacy policies within the context of user privacy values. *IEEE Transactions on Engineering Management, 53*, 227–237.

Galegher, J., Sproull, L., & Kiesler, S. (1998). Legitimacy, authority and community in electronic support groups. *Written Communication*, 15, 493–530.

Gefen, D. (2002). Reflections on the dimensions of trust and trustworthiness among online consumers. *ACM SIGMIS Database, 33*, 38–53.

Green, M. (2007). Trust and social interaction on the Internet. In A. N. Joinson, K. Y. M. McKenna, T. Postmes, & U.-D. Reips (2007). *Oxford Handbook of Internet Psychology* (pp. 43–52). Oxford, UK: Oxford University Press.

Handy, C. (1995). Trust and the virtual organization. *Harvard Business Review, 73*, 40–50.

Harper, J., & Singleton, S. (2001). *With a grain of salt: What consumer privacy surveys don't tell us*. Retrieved on November 29, 2005, from http://www.cei.org/PDFs/with_a_grain_of_salt.pdf.

Heijden, H. V. D., & Verhagen, T. (2002, January). Measuring and assessing online store image: a study of two online bookshops in the Benelux. In *Proceedings of the 35th Annual Hawali International Conference on System Sciences*, Honolulu, Hawali.

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

Holmes, J. G., & Rempel, J. K. (1989). Trust in close relationships. In C. Hendrick (Ed.), *Close relationships* (pp. 187–220). Newbury Park, CA: Sage.

Ingham, R. (1978). Privacy and psychology. In J. B. Young (Ed.), *Privacy* (pp. 35–59). Chichester, UK: Wiley.

Jarvenpaa, S. L., Knoll, K., & Leidner, D. E. (1998). Is anybody out there? Antecedents of trust in global virtual teams. *Journal of Management Information Systems, 14*, 29–64.

Jarvenpaa, S. L., & Tractinsky, N. (1999). Consumer trust in an Internet store: A cross-cultural validation. *Journal of Computer Mediated Communication, 5*(2). Retrieved on October 19, 2007, from http://jcmc.indiana.edu/vol5/issue2/jarvenpaa.html.

Jarvenpaa, S. L., Tractinsky, N., & Vitale, M. (2000). Consumer trust in an Internet store. *Information Management and Technology, 1*, 45–71.

Joinson, A. N. (2001a). Self-disclosure in computer-mediated communication: The role of self-awareness and visual anonymity. *European Journal of Social Psychology, 31*, 177–192.

Joinson, A. N. (2001b). Knowing me, knowing you: Reciprocal self-disclosure on the Internet. *Cyberpsychology & Behavior, 4*, 587–591.

Joinson, A. N., Paine, C. B., Buchanan, T. B, & Reips, U.-R. (under review). *Privacy, trust and self-disclosure online*. Manuscript submitted for publication.

Joinson, A. N., & Reips, U.-D. (2007). Personalized salutation, power of sender and response rates to Web-based survey. *Computers in Human Behavior, 23*, 1372–1383.

Joinson, A. N., Woodley, A., & Reips, U.-D. (2007). Personalization, authentication and self-disclosure in self-administered Internet surveys. *Computers in Human Behavior, 23*, 275–285.

Jupiter Research. (2002). Security and privacy data. Presentation to the Federal Trade Commission Consumer Information Security Workshop. Retrieved on June 20, 2005, from http://www.ftc.gov/bcp/workshops/security/02052011 eathern.pdf.

Larson, D. G., & Chastain, R. L. (1990). Self-concealment: Conceptualization, measurement, and health implications. *Journal of Social and Clinical Psychology, 9*, 439–455.

Liu, C., Marchewka, J. T., Lu, J., & Yu, C.-S. (2005). Beyond concern: A privacy-trust-behavioural intention model of electronic commerce. *Information and Management, 42*, 289–304.

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

Margulis, S. T. (2003). On the status and contribution of Westin's and Altman's theories of privacy. *Journal of Social Issues, 59*, 411–429.

Mayer, R. C., Davis, J. H., & Schoorman, F. D. (1995). An integrative model of organizational trust. *Academy of Management Review 20*, 709–734.

McKenna, K. Y. A., Green, A. S., & Gleason, M. E. J. (2002). Relationship formation on the Internet: What's the big attraction. *Journal of Social Issues, 58*, 9–32.

McKnight, D. H., Cummings, L. L., & Chervany, N. L. (1998). Initial trust formation in new organizational relationships. *Academy of Management Review, 23*, 473–490.

Metzger, M. J. (2004). Privacy, trust and disclosure: Exploring barriers to electronic commerce. *Journal of Computer-Mediated Communication, 9*(4). Retrieved on June 20, 2005, from http://jcmc.indiana.edu/vol9/issue4/metzger.html.

Metzger, M. J. (2006). Effects of site, vendor, and consumer characteristics on web site trust and disclosure. *Communication Research, 33*, 155–179.

Paine, C. B., Joinson, A. N., Reips, U.-D., & Buchanan, T. (2006, September). *Privacy, trust, disclosure and the Internet*. Paper presented to the Association of Internet Researchers (AOIR). Internet Research 7.0: Internet Convergences, Brisbane, Australia.

Paine, C. B., Reips, U.-D., Steiger, S., Joinson, A., & Buchanan, T. (2007). Internet users' perceptions of "privacy concerns" and "privacy actions." *International Journal of Human-Computer Studies, 65*, 526–536.

Parent, W. (1983). Privacy, morality and the law. *Philosophy and Public Affairs, 12*, 269–288.

Parks, M. R., & Floyd, K. (1996). Making friends in cyberspace. *Journal of Communication, 46*, 80–97.

Pew Internet and American Life Project (Fox, S., Rainie, L., Horrigan, J., Lenhart, A., Spooner, T., & Carter, C.). (2001).: *Trust and privacy online: Why Americans want to rewrite the rules*. Retrieved on June 15, 2007, from http://www.pewinternet.org/pdfs/PIP_Trust_Privacy_Report.pdf.

Privacy Knowledge Base (2005). Retrieved on June 20, 2005, from http://privacyknowledgebase.com.

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

Resnick, P., Zeckhauser, R. (2001). Trust among strangers in Internet transactions: empirical analysis of eBay's reputation system. Retrieved on June 1, 2007, from http://www.si.umich.edu/∼presnick/papers/ebayNBER/RZNBER BodegaBay.pdf.

Resnick, P., Zeckhauser, R., Friedman, E., & Kuwabara, K. (2000). Reputation systems. *Communications of the ACM, 43*, 45–48.

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

Rust, R. T., Kannan, P. K., & Peng, N. (2002). The customer economics of Internet privacy. *Journal of the Academy of Marketing Science, 30*, 455–464.

Schatz Byford, K. (1996). Privacy in cyberspace: Constructing a model of privacy for the electronic communications environment. *Rutgers Computer and Technology Law Journal, 24*, 1–74.

Schoeman, F. (1984). Privacy and intimate information. In F. Schoeman (Ed.), *Philosophical dimensions of privacy* (pp. 403–417). Cambridge, UK: Cambridge University Press.

Schoeman, F. (1992). *Privacy and social freedom*. Cambridge, UK: Cambridge University Press.

Smith, H. J., Milberg, S. J., & Burke, S. J. (1996). Information privacy: Measuring individuals' concerns about organizational practices. *MIS Quarterly, 20*, 167–196.

Sparck-Jones, K. (2003). Privacy: What's different now? *Interdisciplinary Science Reviews, 28*, 287–292.

Stewart, K. A., & Segars, A. H. (2002). An empirical examination of the concern for information privacy instrument. *Information Systems Research, 13*, 36–49.

Tanis, M., & Postmes, T. (2007). Two faces of anonymity: Paradoxical effects of Cues to identity in CMC. *Computers in Human Behaviour, 23*, 955–970.

The Guardian (March 15, 2007). *Google to erase information on billions of internet searches*. Retrieved on October 19, 2007, from http://www.guardian.co.uk/technology/2007/mar/15/news.microsoft.

Tidwell, L. C., & Walther, J. B. (2002). Computer-mediated communication effects on disclosure, impressions, and interpersonal evaluations: Getting to know one another a bit at a time. *Human Communication Research, 28*, 317–348.

U.K. Information Commissioner. (2006). *A report on the surveillance society* [online]. Retrieved 27 November, 2006, from http://tinyurl.com/ya76db.

Viseu, A., Clement, A., & Aspinall, J. (2004). Situating privacy online: Complex perceptions and everyday practices. *Information, Communication and Society 7*, 92–114.

Walther, J. B. (1996). Computer-mediated communication: Impersonal, interpersonal, and hyperpersonal interaction. *Communication Research, 23*, 3–43.

Walther, J. B. (1992). Interpersonal effects in computer-mediated interaction: A relational perspective. *Communication Research, 19*, 52–90.

Warren, S., & Brandeis, L. D. (1890). The right to privacy. *Harvard Law Review, 4*, 193–220.

Weiser, M. (1988). Ubiquitous computing. Retrieved on June 20, 2005, from http://sandbox.xerox.com/hypertext/weiser/UbiHome.html.

Westin, A. (1967). *Privacy and freedom*. New York: Atheneum.

Whitty, M. T., & Carr, A. N. (2006). *Cyberspace romance: The psychology of online relationships*. Basingstoke, UK: Palgrave Macmillan.

Whitty, M., & Gavin, J. (2001). Age/sex/location: Uncovering the social cues in the development of online relationships. *CyberPsychology & Behavior, 4*, 623–630.