Computing Handbook
Information Systems and Information Technology
Heikki Topi, Allen Tucker

Privacy, Accuracy, and Accessibility of Digital Business

Publication details
Ryan T. Wright, David W. Wilson
Published online on: 14 May 2014


PLEASE SCROLL DOWN FOR DOCUMENT

Full terms and conditions of use: https://www.routledgehandbooks.com/legal-notices/terms.

This Document PDF may be used for research, teaching and private study purposes. Any substantial or systematic reproductions, re-distribution, re-selling, loan or sub-licensing, systematic supply or distribution in any form to anyone is expressly forbidden.

The publisher does not give any warranty express or implied or make any representation that the contents will be complete or accurate or up to date. The publisher shall not be liable for any loss, actions, claims, proceedings, demand or costs or damages whatsoever or howsoever caused arising directly or indirectly in connection with or arising out of the use of this material.
55

Privacy, Accuracy,
and Accessibility of
Digital Business

55.1 Introduction

Today’s society has been transformed by our ability to do business anywhere using just about any device with Internet connectivity. Digital business refers to the capabilities that make it possible to access information and transact using ubiquitous technologies enabled by the digitization of processes, documents, and services. Technologies facilitating digital business such as cloud computing and mobile access have changed how organizations offer access to information by allowing employees and customers to increase efficiency and task satisfaction by using online tools. As the technology behind digital business has become more and more complex and access become more and more available, severe problems with the security of these systems have emerged.

Many CEOs have ranked security and privacy above financial concerns for their organizations (Boltz 2011). This is not surprising given the publicity surrounding the alleged illicit access to private and sensitive information by several large companies with a strong presence in digital business. Information privacy has also been a major societal/government issue as politicians struggle to protect utility infrastructures that are run using Internet technologies (Bartz 2012). Examining the impact of IT security breaches on privacy, it is evident that this problem is pervasive for both consumers and organizations. For example, Langevin reported that in 2010 cyber-attacks on private information cost nearly $8 billion in the United States (Langevin 2011). Further, over 8 million U.S. residents have been victims
of identity theft due to digital attacks (Langevin 2011). It is clear that information privacy is a serious issue for individuals, organizations, and society in general.

There are typically two pillars to combating digital privacy threats. First, we use security technology (e.g., specialized software) to combat attacking technology (e.g., viruses). The Internet environment has been defended for many years by security systems such as firewalls, virtual private network (VPNs), intrusion detection systems, and so on. On the other hand, the human component of protecting organizations’ and individuals’ privacy looms as an even larger problem. Even the most sophisticated IT security systems can be easily thwarted by human error, incorrect usage, or malicious actions. For example, it was discovered that the Texas government had the private information of over 3 million state workers exposed on the Internet for over a year due to human error (Shannon 2011). Further, in October of 2010 Microsoft servers were commandeered and misused by spammers to promote more than 1000 fraudulent pharmaceutical websites (McMillan 2010). Employee misuse of the systems was again blamed for this security breach.

It is clear that regardless of the technology, the human aspect of information privacy protection remains central in understanding and controlling against breaches, attacks, and misuse. The information systems (IS) discipline should be the right place to address the human–technology–business concerns. IS typically is the interface between business and IT. By providing an understanding of how humans interface with the technology, we can provide a foundation that may help curb information privacy issues. For this reason, the goal of this chapter is to provide a framework to understand the contemporary literature surrounding IS privacy, which is closely tied to the issues of security, and provide a roadmap for future efforts in understanding this important problem of information privacy that threatens digital business. The chapter will focus on the behavioral (as opposed to technical) issues being addressed by IS researchers in the privacy domain.

The chapter will unfold as follows. First, we will define and examine the interplay between information privacy and security. Next, we will provide a foundation for understanding privacy at the individual level. This is then followed by outlining the organizational-level privacy issues. Finally, we will provide a roadmap for future research on privacy and security using the IS research lens.

### 55.2 Defining IS Privacy and Security

It is difficult to explore issues regarding information privacy without discussing security. Many scholars have argued that privacy and security are integrated and are difficult to tease apart (Chan et al. 2005). To this point, Fair Information Practices have been developed that include the intersection of privacy and security. These global principles are guidelines to balance privacy concerns with organizations’ interests (see Table 55.1). This section focuses on the important and significant relationship between privacy and security.

<table>
<thead>
<tr>
<th>Fair Information Practice</th>
<th>Purpose</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Notice</td>
<td>To alert customers to the gathering of their personal information</td>
<td>Your information is collected so we can offer you appropriate goods and services</td>
</tr>
<tr>
<td>Choice</td>
<td>To extend to customers the ability to choose whether their information is tracked, used, and reused</td>
<td>You can choose not to receive e-mails that provide information about sales promotions</td>
</tr>
<tr>
<td>Access</td>
<td>To offer customers access to their personal files to allow them to request that inaccurate information is corrected</td>
<td>You can request the ability to view your file and make any necessary corrections</td>
</tr>
<tr>
<td>Security</td>
<td>To assure customers that their information cannot be accessed by any persons other than those authorized by the organization</td>
<td>We encrypt all information and store it on our secure servers</td>
</tr>
</tbody>
</table>

Companies and individuals have private digital information that they wish to protect from unauthorized access, tampering, corruption, or unplanned disasters. The provision of this protection is referred to as security or, more specifically, information security. The concept of information privacy is rooted in the view that privacy consists of an individual’s control of access to the self (Altman 1975). Accordingly, most modern definitions of information privacy equate privacy with the ability to control one’s private information and others’ access thereto (Smith et al. 2011). A fairly comprehensive definition of this form of privacy is provided by Margulis (1977, p. 10): “Privacy… represents the control of transactions between person(s) and other(s), the ultimate aim of which is to enhance autonomy and/or to minimize vulnerability.”

In the early 2000s, marketing organizations started categorizing end users based on their inherent privacy beliefs (Harris Interactive and Westin 2002). Overall, there are three basic categories:

1. Privacy fundamentalists are the users who do not see any benefit in disclosing any personal or sensitive information. These users are extremely careful of their digital information. According to Harris Interactive, this makes up about 25% of the U.S. population.

2. Privacy pragmatists are those users who undertake a cost–benefit analysis to the collect of their personal information. These users evaluate how organizations are going to use their data and weigh this use with the value of the service. The pragmatists often use cognitive economics risk–reward models to help with their decisions. Harris Interactive predicts that about 55% of the U.S. population consists of privacy pragmatists.

3. Privacy unworried are users who are unconcerned in general with how organizations use their personal information. This group generally rejects others’ view that there are concerns with personal information. Harris Interaction classifies about 20% of the U.S. population as unworried.

Companies’ and individuals’ need for security is driven by a desire for one of several privacy concerns, though the relationship between privacy and security is debated in the literature (Belanger et al. 2002). Culnan and Williams (2009) argue that even when organizations take sufficient precautions in protecting personal information (thus providing information security), they might still engage in or permit unauthorized use of that information, which violates users’ information privacy. Thus, as Ackerman (2004) states, “security is necessary for privacy, but security is not sufficient to safeguard against subsequent use, to minimize the risk of… disclosure, or to reassure users” (p. 432, cf. Smith et al. 2011). The next section will outline the mechanisms used to understand a user’s expectations for security and privacy.

55.2.1 Protecting Users

Protecting users’ privacy with security measures is the nexus of understanding both security and privacy issues. This protection is accomplished through providing three security assurances to the end users of an IS: (1) integrity, (2) confidentiality, and (3) authentication (Smith et al. 2011). Taken together, the security assurances provide a framework for end users and organizations to understand the mechanics involved in information security. Since our focus is on the human factors involved in protecting users’ privacy, we will break down each assurance in terms of possible threats and opportunities for knowledge advancement (See Table 55.2). In order to do so, we will integrate Smith et al.’s conceptualization of security assurances with Smith et al.’s (1996) research on an individual’s information privacy concerns or concern for information privacy (CFIP).

Smith et al.’s (2011) conceptualization of security can be likened to an onion where each assurance is based on the previous order of assurance. Core to the assurance model is integrity. The next layer is confidentiality and finally authentication. With this layered approach, in order to create problems with one of the assurances, the previous assurance must be compromised. For example, if the confidentiality of the private information is inappropriately leaked, first authentication must have been compromised. This is a general rule of thumb when conceptualizing how security threats affect the assurances (see Figure 55.1).
The following section discusses the ways in which the three security assurances provide protection of users’ private information. We discuss each of the aspects of Stewart and Segars’ (2002) information privacy concerns research. These concerns are summarized in the first column of Table 55.1, which also includes definitions and human threats for each of the three categories of privacy concerns. Table 55.1 also maps these privacy concerns to each of the three security assurances illustrated in Figure 55.1. We now proceed to discuss each grouping of privacy concerns and security assurances in turn, addressing first the privacy concerns, then explaining the related security assurance.

### 55.2.2 Privacy: Collection and Errors

The collection and accuracy of private information are one potential source of users’ concerns regarding information privacy (Stewart and Segars 2002). The act of collecting private information inherently reduces an individual’s control over that information, since the individual no longer has direct oversight regarding the information collected. Collection concerns focus on both the amount of personal information being collected and how the information is being stored (Culnan and Bies 2003; Malhotra et al. 2004a). Error concerns are based on the protection against deliberate and accidental error in personal data (Smith et al. 1996). Though the Smith et al. (1996) model separates collection and information errors, these two are often discussed together since most errors in IS take
place during a collection process (Clouse et al. 2010). And, in the context of our security assurance framework, both collecting private information and ensuring that it is free from error are related to integrity, as discussed next.

55.2.3 Security: Integrity

Integrity provides assurance that collected private information is not altered during transit or storage. There are two significant human threats associated with integrity. The first threat associated with human interactions is information accuracy. Information accuracy entails ensuring that the fidelity of information stays intact. Security issues often occur when users (or hackers) change data. Hospitals are often faced with accuracy problems as small changes by medical staff in electronic medical records can cause major patient problems and even result in death (Cliff 2012). The second factor that can be manipulated by humans is information reliability. Information reliability is a product of how the users view the information provided by a system. In many instances, we have seen a user question the system’s reliability and therefore ignore system requests or system information when making important decisions. One such example is seen in research done on Microsoft’s anti-phishing toolbar (Wu et al. 2006). In this study, it was shown that the information provided by the system—in this case the anti-phishing toolbar—was unreliable less than 10% of the time. However, this unreliable information caused users to disregard the information provided by the tool altogether, causing a security threat.

55.2.4 Privacy: Secondary Use

The application of confidentiality in privacy is mainly concerned with the secondary use of data. This may include selling of personal information, marketing using personal information, using personal information to make business decisions, and so on. Although explicit research on secondary use of information is scant, there has been a great deal of popular press about this issue. For example, in late 2011 Google changed their data privacy statement (Garside 2012). This change in policy gained much attention, as Google owns a lot of personal information about their users. It is clear that Google benefits when aggregating personal information from their different businesses. For example, Google can aggregate private information about which videos a user watches from YouTube with geo-location information from their Android phone while scanning the user’s Gmail account for certain key words. Using this aggregated data Google can clearly distinguish market segments at a very fine level of detail.

The concerns of users regarding tracking of their online behavior have caused government bodies to start regulating the use of tracking technology such as “cookies,” which are text files used to track Internet browsing behavior. In one such case, the European Union’s 2011 online privacy law now makes it very difficult for marketers to capture users’ information by directing online companies such as Microsoft and Google to add a “do not track” button to their web browsing software (Enright 2012).

There are two main points of emphasis when addressing privacy concerns surrounding secondary use. First is the issue of control by the user of information access by other parties. Control in this instance means that users desire control over who sees what particular piece of personal information. For example, the “do not track” button on browsers allows users to control which information is captured. The second issue is awareness (what Chan et al. 2005 classify as “Notice”). Awareness is the individual’s desire to be accurately informed regarding the extent to which the organization shares his or her personal information with third parties. One of the biggest issues for consumers is whether the organization will be allowed to sell this personal information to interested third parties. Being in control and aware in order to reduce users’ concerns regarding secondary use requires that organizations manage confidentiality.
55.2.5 Security: Confidentiality
Confidentiality ensures that information is disclosed only to authorized individuals and for authorized purposes. The research around confidentiality in general is difficult to execute due to its sensitive nature. The core threat issue has to do with information property. Information property focuses on who owns the personal information and how this information can be exchanged (Litman 2000).

55.2.6 Privacy: Unauthorized Access
It is clear that access to information is critical to knowledge workers and decision makers in an organization. However, unlimited access to information is a concern as it increases the likelihood of breaches, leaks, and misuse of private information (Malhotra et al. 2004a). As with most security decisions, and as previously mentioned, there is commonly a risk–reward decision pertaining to privacy. With authentication and control these questions are as follows:

1. Who should access the information?
2. For what purpose do they need access?
3. How is this information being used?
4. When do they need access to this information?

These questions most definitively are associated with privacy concerns. Privacy concerns about improper access include trepidations that personal data are readily available to users that are not authorized to access, use, or disclose the personal information (Smith et al. 1996). Understanding users’ desire for protection against unauthorized access to private information is a critical security issue that needs to be addressed by the IS authentication process.

55.2.7 Security: Authentication
Authentication provides verification of one’s identity and permission to access a given piece of information. Authentication is sometimes seen as a mechanical process whereby a system either provides access or not. Authentication processes are typically set by policies and business rules and enforced by automated systems to provide access to personal or sensitive information. The concept of users’ accessibility is the human threat in this assurance category. The concept of information accessibility has been around since the early 1980s. Information accessibility is defined as what information a person or organization has the right to obtain about others and how this information can be accessed and used (Culnan 1984). Accessibility, which is enforced by authentication, is a critical issue for IS managers. Seminal research has posited a positive relationship between perceived accessibility of information and the information use (Culnan and Armstrong 1999).

The next two sections will build on the privacy concerns and security assurances explored earlier to give some guidance on how individual behaviors can influence security behavior. This is followed by scrutinizing how these individual behaviors influence organizational policies and procedures.

55.3 Privacy Behaviors
As the pivotal factor in considering information privacy, humans have been the object of a plethora of privacy and security research and theories in the IS discipline. Organizational policy and outcomes are undoubtedly linked to individual behaviors. Thus, we first synthesize and summarize the literature concerning individual behavior related to information privacy and security. These topics and sample studies are summarized in Table 55.3.
Privacy, Accuracy, and Accessibility of Digital Business

55.3 Theories about Perceptual Beliefs

Much of the IS literature that surrounds privacy and security has been based on individuals’ perceptions of certain behaviors that have been developed in conjunction with privacy and security theories. Some examples of research questions about individuals’ perceptions are as follows: (1) Do you trust people online (McKnight et al. 2011)? (2) How private do you need to keep your sensitive information (Dinev and Hart 2004, 2006)? (3) How concerned are you about disclosing personal information (Malhotra et al. 2004b)? All of this research uses an individual lens of analysis to understand how users’ beliefs impact their interactions with technology systems such as

<table>
<thead>
<tr>
<th>Theories</th>
<th>Description</th>
<th>Sample Studies</th>
</tr>
</thead>
<tbody>
<tr>
<td>Trust and risk literature</td>
<td>Common constructs included in theories modeling individual security and privacy behavior. These serve to facilitate or inhibit secure behavior and/or information disclosure</td>
<td><em>Trust and distrust</em> (Gefen et al. 2008; McKnight and Choudhury 2006; McKnight et al. 2002)</td>
</tr>
<tr>
<td></td>
<td></td>
<td><em>Risks</em> (Dinev and Hart 2006; Featherman and Pavlou 2003; Gabriel and Nyshadham 2008; Pavlou and Gefen 2004)</td>
</tr>
<tr>
<td>Protection-motivation theory</td>
<td>Self-protection theory adapted from the health behavior domain, which argues that secure behavior is motivated by perceptions of vulnerability, severity of threat, and the effectiveness or efficacy of secure behavior</td>
<td>(Herath and Rao 2009b; Johnston and Warkentin 2010; Lee and Larsen 2009; Ng et al. 2009)</td>
</tr>
<tr>
<td>Deterrence theory</td>
<td>Theory adapted from criminology that predicts the effectiveness of sanctions on users’ secure behavior. The theory generally concerns a sanction’s severity and certainty</td>
<td>(D’Arcy et al. 2009; Harrington 1996; Herath and Rao 2009a; Kankanhalli et al. 2003; Pahnila et al. 2007; Straub 1990)</td>
</tr>
<tr>
<td>Neutralization/rational choice</td>
<td>Theoretical lens that accounts for users who justify or neutralize their insecure behavior and/or rationally decide to behave insecurely after weighing the costs and benefits of secure behavior</td>
<td>(Li et al. 2010; Siponen and Vance 2010)</td>
</tr>
<tr>
<td>Theory of planned behavior</td>
<td>Common cross-disciplinary theory that predicts a person’s behavior according to behavioral intentions, which are influenced by attitudes, social norms, and perceptions of self-efficacy or behavioral control. This has been used as a framework to explain different aspects of security compliance and other individual behaviors</td>
<td>(Ajzen 1991; Bulgurcu et al. 2010; Dinev and Hu 2007)</td>
</tr>
<tr>
<td>Privacy disclosure</td>
<td>Rich stream of literature that investigates privacy disclosure behavior, both from the perspective of the organization trying to encourage disclosure for marketing and other purposes and from the perspective of the user who would rather not disclose much information in order to protect privacy</td>
<td>(Acquisti and Grossklags 2005a; Chellappa and Sin 2005; Li et al. 2011; Lu et al. 2004; Malhotra et al. 2004a; Smith et al. 1996; Tsai et al. 2011; Xu et al. 2011)</td>
</tr>
</tbody>
</table>
Managing and Securing the IT Infrastructure and Systems

e-commerce, enterprise resource planning (ERP), and so on. The following will outline the three main theoretical perspectives and their respective individual-level behavioral perceptions related to privacy.

55.3.1.1 Risks

In the context of privacy, risk has been defined as “the degree to which an individual believes that a high potential for loss is associated with the release of personal information to a firm” (Smith et al. 2011, p. 13). Perceived risks are often characterized as one’s sense of control over their personal information (Featherman and Pavlou 2003), or the general beliefs one has about the likelihood of organizations sharing that information (whether intentionally or through insufficient security precautions) with unauthorized third parties (Dinev and Hart 2006). Risks can either be associated with a specific transaction or transaction partner (Li et al. 2011; Slyke et al. 2006) or refer to a general measure of risks associated with transacting via the Internet (Dinev and Hart 2006; Gabriel and Nyshadham 2008). When the likelihood of unauthorized sharing or security breaches is perceived to be high, individuals tend to report higher privacy-related concerns (Dinev and Hart 2004, 2006), are less trusting of the organization (Pavlou and Gefen 2004), and are accordingly less willing to conduct transactions with that organization (Pavlou and Gefen 2004).

55.3.1.2 Concerns

Closely related to privacy and security risks, privacy concerns reflect users’ worries about the potential loss of information privacy (Xu et al. 2011). Just as with privacy risks, privacy concerns have been framed both at the general level reflecting broad concerns about electronic transactions (Dinev and Hart 2006; Li et al. 2011; Slyke et al. 2006) and at the situation level representing specific concerns about a given transaction or transaction partner (Xu et al. 2011). Privacy concerns have become the default measurement proxy for measuring users’ beliefs or attitudes about privacy in general (Smith et al. 2011). Not surprisingly, individuals who report higher privacy concerns, either at the general or at the specific level, perceive privacy risks to be higher (Li et al. 2011; Malhotra et al. 2004a) and are less willing to engage in transactions via the Internet (Dinev and Hart 2006).

55.3.1.3 Trust

Underlying several of the concepts in this section, trust has been validated as key in facilitating online interactions, both in e-commerce (McKnight et al. 2002) and other (e.g., Posey et al. 2010) contexts. Trust is a many-faceted topic, around which a vast literature has developed. As such, it is beyond the scope of this chapter to provide detailed treatment of the topic. We will thus briefly summarize the trust literature, particularly with respect to the interrelationships between trust and the privacy and security concepts.

McKnight et al. (2002), building on earlier work in off-line contexts (Mayer et al. 1995; McKnight et al. 1998), proposed the most popular framework for online trust formation. This model proposes that trusting beliefs about an entity’s benevolence, integrity, and competence will predict the extent to which a user will be willing to transact with the entity. The recipient of trust in the majority of prior research is an e-commerce company (e.g., Pavlou and Gefen 2004), but a growing body of research investigates trust from other perspectives such as social media (Lankton and McKnight 2012), productivity software (Lankton and McKnight 2011; McKnight et al. 2011), and knowledge management systems (Thatcher et al. 2011).

Trust has been shown to be an important part of our understanding of privacy and security in online settings. Trust has been shown to predict feelings of privacy (Belanger et al. 2002), but has more often been modeled as an outcome of privacy (Chellappa and Sin 2005; Malhotra et al. 2004a), wherein a reduction of privacy concerns has been associated with higher levels of trust. Schoenbachler and Gordon (2002) showed that when consumers trust companies, they show lower concern for privacy and are more willing to provide personal information (cf. Smith et al. 2011).
55.3.1.4 Distrust

A concept that is related to but distinct from trust is distrust. Rather than assuming trust and distrust to be two extremes on a singular continuum (Rotter 1980), a mounting body of research is finding that the thought patterns underlying trust and distrust are distinct (Dimoka 2010; McKnight and Choudhury 2006). Trust tends to build slowly, with organizations and online services expending great effort to engender trust among their users (Kim and Benbasat 2003). When trust is violated, however, it is “shattered, and it is replaced with a totally different mind-set, what [we call] distrust” (Gefen et al. 2008, p. 278). Research on distrust in the context of privacy and security remains sparse, with the literature firmly focused on the relationships with trust. As with the e-commerce literature, however, differentiating between trust and distrust in the context of privacy and security can yield more valuable and unique understanding than a focus on trust alone can afford (Gefen et al. 2008).

55.3.2 Theories about Compliance Behaviors

Security compliance behavior has been a popular topic in the IS literature, particularly in the last decade. Compliance research generally deals with factors that predict end-user compliance with organizational privacy and security policies (e.g., Bulgurcu et al. 2010), but has also been examined in home security settings, which impact one’s exposure to privacy issues (Anderson and Agarwal 2010). A number of theoretical perspectives have been leveraged to explain compliance behavior. We will address each in turn.

55.3.2.1 Protection-Motivation Theory/Health Belief Model

Researchers have adapted the popular protection-motivation theory (PMT; Rogers 1983) to explain why users adopt secure behavior. Closely related are the health belief model (Rosenstock 1966) and the technology threat avoidance theory (Liang and Xue 2010), the latter of which was recently developed in the IS literature as a partial extension of PMT. These theories treat security threats as hazards about which individuals make judgments regarding such factors as threat severity, perceived vulnerability, the efficacy of suggested protections, or the ability of the individual to carry out those protections. Secure behavior is thus treated similar to healthy eating or exercise habits, with individuals varying in their respective judgments of how dangerous security threats are or how vulnerable they are to being compromised in some way. These theories have been used extensively in the IS security compliance literature, in some cases directly (e.g., Herath and Rao 2009b; Johnston and Warkentin 2010; Lee and Larsen 2009; Ng et al. 2009) and in others less as a framework and more as support for individual hypotheses (e.g., Bulgurcu et al. 2010; Pahnila et al. 2007).

55.3.2.2 Deterrence Theory

A large body of IS literature has investigated the effects of punishments or sanctions in motivating individuals to adhere to organizational security policies and behave securely. The facets of sanctions that have generally been explored include severity (how harsh the punishment will be) and certainty (the perceived probability that punishment will be given) (e.g., Straub 1990). Deterrents have been found to be effective in minimizing security violations in organizational (D’Arcy et al. 2009; Harrington 1996; Herath and Rao 2009a; Kankanhalli et al. 2003; Pahnila et al. 2007) and other (Straub and Welke 1998) settings.

55.3.2.3 Neutralization/Rational Choice

Recent expansion beyond the deterrence literature has introduced new perspectives to the issues associated with end-user behavior. One such perspective acknowledges that deterrence mechanisms are effective in many contexts, but that users will occasionally rationalize or neutralize their insecure behavior even in the presence of imposed sanctions (Siponen and Vance 2010), or that users deliberately choose...
to act insecurely after weighing the costs of following security policies against the benefits of disregarding them (Li et al. 2010). These perspectives have been validated empirically, and they offer a fresh understanding of the compliance issues that complement the findings regarding the effectiveness of deterrence mechanisms.

**55.3.2.4 Theory of Planned Behavior**

Several frameworks have been proposed in the IS literature that attempt to frame users' intentions according to the theory of planned behavior (TPB; Ajzen 1991). Dinev and Hu (2007) use the TPB to explore users' intentions to adopt protective technologies. Bulgurcu et al. (2010) frame the idea of information security awareness within the TPB and theoretically justify a comprehensive framework that explains the outcomes of information security awareness and how they relate to a user's behavioral intentions regarding secure behavior.

**55.3.3 Privacy Disclosure Behaviors**

Research regarding privacy disclosure behaviors generally falls into one of two approaches. The first takes the side of the e-commerce company that would like as much information from its customers and potential customers as it can legally acquire, since such personalized information is highly valuable to for marketing and other business applications (Chellappa and Sin 2005; Lu et al. 2004; Xu et al. 2011). Furthermore, for e-commerce companies to gain revenues, their customers must generally supply at least a minimal amount of personal information (e.g., credit card or shipping information) in order to complete a transaction. Thus, this body of research investigates ways to mitigate privacy concerns so as to facilitate as much sharing of private information by the consumer as possible.

For example, Chellappa and Sin (2005) studied the likelihood of users to supply personal information in exchange for personalized browsing experiences, and trust building factors were proposed to mitigate users’ privacy concerns. Lu et al. (2004) proposed using what they call social adjustment benefits (a type of social psychological motivation) to motivate users to disclose information to enable companies to pursue a strategy of focused marketing. In a more recent study (Xu et al. 2011), monetary compensation and multiple forms of industry regulation were proposed as factors that would both increase perceived benefits and reduce perceived risks of disclosing information to location-aware mobile services. In these examples, the objective is to maximize information disclosure for the benefit of the company.

The other dominant approach takes the side of the consumer in defending them against too-frequent or too-generous privacy disclosure behavior. This literature is focused on the so-called privacy paradox (Acquisti 2004; Acquisti and Grossklags 2003, 2005a,b; Norberg et al. 2007), wherein individuals state salient concerns about privacy and sharing private information, but proceed to behave in ways contrary to their stated beliefs (Norberg et al. 2007). Acquisti and colleagues (Acquisti 2004; Acquisti and Grossklags 2003, 2005a,b; Tsai et al. 2011) have investigated probable causes of this contradictory behavior. Their work serves as an example of research that seeks to benefit the users in protecting them from overgenerous disclosure behavior. They address the issue from a behavioral economics perspective and suggest that the privacy paradox is the result of such limitations as psychological distortions (e.g., hyperbolic discounting of risks), limited or asymmetrical information (because of which users do not know the full implications of disclosure), and bounded rationality (i.e., the inability to accurately process all of the probabilities and amounts of benefits and costs related to privacy disclosure) (Acquisti and Grossklags 2003). It is possibly because of these limitations that users have the tendency to give up private information in return for relatively small conveniences or rewards, even when their stated privacy concerns do not support this behavior. This irrational behavior is generally framed negatively. For example, Tsai et al. (2011) show that when privacy policies are made more obvious and accessible (thus reducing information asymmetries), users tend to act more securely and reduce their disclosure behavior.
55.3.4 Privacy Issues with Deception and Fraud in the Twenty-First Century

When privacy is violated or security breaks down, the results can be far-reaching. Businesses lose billions of dollars each year due to cyber-attacks (Langevin 2011), and our increasingly socially networked world has introduced a new generation of privacy issues (Vaidhyanathan 2011). For example, there are more and more attacks via social networks that directly target individuals (Lewis and Kaufman 2008). This section addresses several topics related to security or privacy threats, as well as some countermeasures that are being developed to reduce those threats.

Though deception and fraud are age-old traditions of the human race, these have become increasingly nuanced since the advent of the Internet and electronic communications, with direct impacts on information security and privacy. Deception, which has been defined (Buller and Burgoon 1996) as “a message knowingly transmitted by a sender to foster a false belief or conclusion by the receiver,” can take many forms. These range from impression management activities and half-truths to outright lies and financial fraud. Deception and fraud mediated through electronic channels have major implications for both traditional and digital businesses, as well as for individual consumers.

One common way in which deception and fraud can occur is in relation to products sold by online retailers. This type of deception has been called product-related deception, which is when online merchants deliberately manipulate product-related information with the intent to mislead customers (Xiao and Benbasat 2011). Though product-related deception is not unique to online channels, customers shopping online have fewer cues with which to recognize deception. This makes Internet users more vulnerable to deceptive practices such as product misrepresentation, nondelivery of products, obfuscation of warranty or refund policies, or misuse of personal or financial information (Pavlou and Gefen 2005; Xiao and Benbasat 2011).

Fraudsters seeking to gain financially from their deception have found that the Internet provides many opportunities for financial fraud perpetrated against individual users. One of the more popular schemes involves what is known as phishing. In this type of scam, the “phishers” create an e-mail that mimics the look and feel of a legitimate business and asks the user to visit a website to correct some purported technical error. A link is provided that takes them to a fraudulent website constructed to match the legitimate website in every way possible. If an inattentive user attempts to sign in to the website, the phishers are able to obtain the person’s username and password, which can then be used to defraud him or her with full online account access.

With phishing, we see a direct relationship between individual-level privacy beliefs and security practices. Phishing is indeed a direct attack on one’s online privacy. Unfortunately, research on phishing and related online deception is somewhat sparse. Dhamija et al. (2006) investigated various individual characteristics, including gender, age, computer experience, or education. They found no significant differences in the ability of users to detect deception in fraudulent websites. In a series of studies (Wright et al. 2010; Wright and Marett 2010), students were experimentally phished for private information, and the researchers then accounted for both experiential factors (e.g., computer self-efficacy, web experience) and dispositional factors (e.g., trust, suspicion) in determining whether the deceiver was successful in phishing the sensitive information from the student. The results show that while both sets of factors play a role in how effective a phishing scam will be, experiential factors had a stronger influence on the outcome of the deception. In terms of privacy, the behavioral aspect of information disclosure adds to the complexity when trying to guard against attacks on private or personal information.

55.3.4.1 Countermeasures

To counteract the exponential rise of online fraud and deception (e.g., Gyongyi and Garcia-Molina 2005), systems have been developed with the specific purpose of alerting users to fake or otherwise fraudulent websites. In other words, privacy alerts are now a part of many automated systems.
Currently, these systems vary in sophistication and effectiveness, and users tend to discount their usefulness and avoid adoption (Wu et al. 2006).

Most fraud detection systems use a lookup or classification strategy (Abbasi et al. 2010). A lookup strategy consists of a small client (usually a browser toolbar installed on the user’s machine) that connects to a repository of known fraudulent websites (i.e., a blacklist) and then warns the user before a black-listed site is accessed (Wu et al. 2006; Zhang et al. 2007). A classifier system uses characteristics of the website itself to classify the site as either safe or fraudulent, according to rule-based heuristics (Zhang et al. 2007). These characteristics include such cues as domain name, host country, or content similarity (compared to frequently spoofed sites such as eBay or PayPal) (Abbasi et al. 2010). These lookup- or classification-based systems are generally ineffective, with reported accuracy rates of 70% or lower (Abbasi et al. 2010; Zhang et al. 2007).

Recent advances in automated fraud detection systems (e.g., privacy attack systems) have been embodied in a new fraud detection system proposed by Abassi et al. (2010). This system utilizes a statistical learning theory approach to analyze a wider set of cues and domain-specific knowledge. The authors demonstrate that this more advanced detection method outperforms other, less sophisticated systems. Although this and other fraud detection systems have not been heavily adopted by the general public, advancements in this area are encouraging and should help to combat the pervasive fraudulent activity on the Internet. Reducing the incidence of successful phishing and other fraudulent activity should be a primary focus in further protecting users’ information privacy.

55.3.4.2 Organizational Issues

Organizations play a pivotal role in the information privacy and security discussion. This is because organizations are primarily charged with protecting individuals’ information privacy, either in protecting employees’ financial or other personal information, or in protecting the private information they collect about their customers or clients in the course of doing business. A transaction in which an organization acquires any form of private information from a customer must, as a precondition, engender enough trust or goodwill such that the customer is comfortable with the risk of releasing that information to the organization. Culnan and Bies (2003) argue that any disclosure of personal information constitutes an assumption of risk on the part of the consumer. Recall that security is a necessary but insufficient condition for protection of privacy (Ackerman 2004), since privacy entails the added assurance that an individual’s private information will not be used in a way other than originally intended by the sharer of that information, nor shared with unauthorized third parties (Culnan and Williams 2009).

Given the organizations’ responsibility to protect their stakeholders’ privacy, information security has become a critical topic for organizations. Researchers have noted vital financial and legal implications for failing to protect information privacy (Goel and Shawky 2009; Gordon and Loeb 2002). It has also been proposed that a majority of organizational security issues are related to human error or noncompliance with security policies (Stanton et al. 2005). Accordingly, organizations have reported employees’ security-related behavior as a top concern for years (Boltz 2011). The issues that organizations cope with, and the countermeasures that they implement, thus result from tendencies of their employees’ individual behaviors.

55.3.5 Security Policies/Compliance

As concerns regarding privacy and security have increased, organizations have implemented privacy and security policies to help inform employees of standards and to enforce security precautions where necessary to ensure the privacy of the organization’s data and employees. Hone and Eloff (2002) identify the information privacy and security policy, the most singularly important security control that an organization can implement. This view is also shared by others (Knapp et al. 2009; Whitman 2008).

An information privacy and security policy is established to provide management direction and support for information privacy and security as derived from business requirements and relevant laws and
regulations (Knapp et al. 2009). Policies generally consist of a general objective or purpose, a stated scope indicating to whom the policy applies, assigned responsibilities where various organizational roles are given ownership over various portions of the policy, and guidelines for compliance, which provide for the policy’s enforcement (Olzak 2006). These are general guidelines that vary according to an organization's needs.

That an entire body of literature (noted earlier) has developed around employee noncompliance with security policies is an indication that many policies or portions of policies are not regularly followed by employees. This represents a serious problem for organizations, since noncompliance by even a few employees can largely negate the benefits of even the most stringent of policies. Organizations must strike a balance between instituting policies that are overly restrictive, which can lower productivity or instill contempt among annoyed employees, and policies that are not restrictive enough, which largely defeats the purpose of a security policy. This balance is elusive, and privacy and security policy compliance continues to fuel discussion and investigation in the literature.

### 55.3.6 Legal Requirements (SOX, GAAP, Others)

Following the several cases of corporate accounting fraud shortly after the turn of the century, the most notable of which were the Enron and WorldCom scandals, the U.S. government enacted legislation designed to close accounting loopholes and generally tighten controls on accounting practices. This legislation, termed the Sarbanes-Oxley (SOX) Act, has had far-reaching effects, many of which have directly impacted the IS function in many organizations (Volonino et al. 2004). Among the requirements detailed in the SOX bill, companies must ensure transparency, accuracy, timeliness, and reliability of their IT-enabled financial reporting and operations systems. These requirements necessitate security policies and managerial oversight to ensure employee compliance with those policies. Indeed, Volonino et al. (2004) state that “to be in compliance with regulatory boards, companies need to develop and deploy effective information security response and investigation policies. Those policies will require collaboration between corporate IT security teams and IT auditors” (p. 226).

In summary, organizations have the responsibility to ensure the security and privacy of their employees and customers. To accomplish this, most organizations employ official policies requiring certain levels of private and secure behavior. Though noncompliance with these policies is the object of considerable research in the literature, organizations continue to strive to provide for their stakeholders’ privacy and security.

### 55.4 Future Research Agendas

This chapter has identified the major theoretical perspectives and some current privacy- and security-related problems and solutions. Clearly, there are many associated research opportunities that IS scholars can address. The following will outline three areas within privacy and security that we believe have the potential to impact end users, organizations, and society in general. We will first explore interesting questions in the design for privacy and security.

#### 55.4.1 Designing for Privacy and Security

Consistent with the theme of individual behaviors that persists in this chapter, we will look toward design as an avenue that affects privacy and security for individuals. Specifically, we will address the balance between allowing end users to act and automating privacy and security tasks. Within application design, security tools have either focused on being invisible (e.g., filters, automated messages, and so on) or attaching attention (e.g., call outs, security alerts, and so on) (Hong 2012). Although there are mixed results, what is clear is that no single method can achieve the results needed for 100% secure practices that ensure one’s privacy. Further, since privacy is individually constructed, one system run by homogenous business rules would likely meet with user resistance or nonadoption. For this reason, the first step
toward understanding the design elements for secure IT systems is to develop a framework that includes the invisible (e.g., automatic systems) and the visible (e.g., warnings and human decision points). The need for this framework is echoed in Sheng et al.’s (2010) phishing research, which identifies clear gaps between the heuristics (e.g., the decision process for end users) and machine-learning algorithms (e.g., anti-phishing toolbars). Other general privacy and security research has followed this pattern. In order to solve complex phenomena such as privacy and security issues, it will take a multidisciplinary effort from psychologists, computer scientists, and IS scholars. With multidisciplinary efforts, we will be able to address significant privacy and security questions that are as follows:

1. What privacy decisions are best made using machine learning and which are best left to humans?
2. How should machine-learning algorithms interact with end users?
3. Is there a theoretical perspective that could integrate the need for visibility and invisibility of certain processes?

By attempting to address these questions, the privacy researchers should coalesce around common themes within this important domain.

### 55.4.2 Understanding Training

Training has been posited as the main defense against directed attacks (Hong 2012). In fact, there has been a variety of training experiments by the anti-phishing group at Carnegie Mellon University (CMU) (Kumaraguru et al. 2009; Sheng et al. 2010). Hong states that “it doesn’t matter how many firewalls, encryption software, certificates, or two-factor authentication mechanisms an organization has if the person behind the keyboard falls for a phish” (Hong 2012, p. 76). Training against phishing has taken two lines. First, the CMU group and others have designed microgames that teach employees how to spot phishing messages (Sheng et al. 2007). The second is embedded training in which participants are sent phishing messages in a classroom setting and are asked to evaluate these. Kumaraguru et al. (2009) found this approach to be effective even a month after training. These phishing training mechanisms may offer other areas a clear path for implementation. Some questions around privacy and security include the following:

1. Are some training techniques better than others (e.g., mindfulness training, cognitive trainings)?
2. What are the best delivery mechanisms for training (e.g., online, classroom, games)?
3. How do you combine privacy and security training?
4. What are the biggest gaps in training for employees? For consumers?

Obviously, there are many other opportunities for training research that can be considered. It is important first to address the big IS questions using a multidisciplinary point of view and expertise as stated earlier.

### 55.4.3 Looking at Information Systems’ Policy Differently

A lot of attention is currently paid to employee compliance with privacy and security policies (Hone and Eloff 2002; Knapp et al. 2009; Whitman 2008). In fact, most of the theoretical work is geared toward understanding why an organization’s personnel comply with the policy or not (e.g., PMT, deterrence theory, and so on). What is not clear is how the policy itself may enact certain behaviors from employees and consumers. The following research questions are appropriate starting points to address how policy affects behavior:

1. Is there a better way to classify the interplay between IS security policies and privacy beliefs?
2. What is the impact of less-restrictive IS polices on the work force?
3. How do privacy and security policies impact productivity?
4. Do privacy policies influence e-commerce interactions?
In sum, there are multiple interesting angles from which to study privacy and security policy issues that are yet to be explored. These and others represent excellent opportunities for future knowledge creation.

55.5 Conclusion

This chapter outlines the current issues with information privacy and security. In doing so, we have provided a framework that summarizes the interplay between users’ concerns regarding information privacy and the provision of that privacy through the three basic components of security assurance: (1) authentication, (2) confidentiality, and (3) integrity. Further, we provide the current state of research at the individual and organizational levels of analysis. Finally, we identify three gaps in privacy and security research that IS scholars should address (i.e., design issues, training, and policies).

References


Boltz, M. 2011. Top three security concerns every CEO should know, (available at http://chiefexecutive.net/top-three-security-concerns-every-ceo-should-know [accessed on March 24, 2013]).


Culnan, M. J. The dimensions of accessibility to online information: Implications for implementing office information systems, ACM Transactions on Information Systems (2:2) 1984, 141–150.


Culnan, M. J. and Williams, C. C. How ethics can enhance organizational privacy: Lessons from the choicepoint and TJX data breaches, MIS Quarterly (33:4) 2009, 673–687.


Dimoka, A. What does the brain tell us about trust and distrust? Evidence from a functional neuroimaging study, MIS Quarterly (34:2) 2010, 373–396.


Li, H., Sarathy, R., and Xu, H. The role of affect and cognition on online consumers’ decision to disclose personal information to unfamiliar online vendors, *Decision Support Systems* (51:3) 2011, 434.


Privacy, Accuracy, and Accessibility of Digital Business


