MIS Quarterly

THEORY AND REVIEW

INFORMATION PRIVACY RESEARCH: AN INTERDISCIPLINARY REVIEW[1]

H. Jeff Smith
Department of Decision Sciences and Management Information Systems, Farmer School of Business, Miami University, Oxford, OH 45056 U.S.A. {jeff.smith@muohio.edu}

Tamara Dinev
Department of Information Technology & Operations Management, College of Business, Florida Atlantic University, Boca Raton, FL 33431 U.S.A. {tdinev@fau.edu}

Heng Xu
College of Information Sciences and Technology, Pennsylvania State University, University Park, PA 16802 U.S.A. {hxu@ist.psu.edu}

To date, many important threads of information privacy research have developed, but these threads have not been woven together into a cohesive fabric. This paper provides an interdisciplinary review of privacy-related research in order to enable a more cohesive treatment. With a sample of 320 privacy articles and 128 books and book sections, we classify previous literature in two ways: (1) using an ethics-based nomenclature of normative, purely descriptive, and empirically descriptive, and (2) based on their level of analysis: individual, group, organizational, and societal.

Based upon our analyses via these two classification approaches, we identify three major areas in which previous research contributions reside: the conceptualization of information privacy, the relationship between information privacy and other constructs, and the contextual nature of these relationships.

As we consider these major areas, we draw three overarching conclusions. First, there are many theoretical developments in the body of normative and purely descriptive studies that have not been addressed in empirical research on privacy. Rigorous studies that either trace processes associated with, or test implied assertions from, these value-laden arguments could add great value. Second, some of the levels of analysis have received less attention in certain contexts than have others in the research to date. Future empirical studies—both positivist and interpretive—could profitably be targeted to these under-researched levels of analysis. Third, positivist empirical studies will add the greatest value if they focus on antecedents to privacy concerns and on actual outcomes. In that light, we recommend that researchers be alert to an overarching macro model that we term APCO (Antecedents → Privacy Concerns → Outcomes).

Keywords: Information privacy, multi-theory, regulation, society, interdisciplinary

[1]M. Lynne Markus was the accepting senior editor for this paper. Paul Pavlou served as the associate editor.

The appendices for this paper are located in the "Online Supplements" section of the *MIS Quarterly*'s website (http://www.misq.org).

Introduction

Information privacy is of growing concern to multiple stakeholders including business leaders, privacy activists, scholars, government regulators, and individual consumers. Public opinion polls report that privacy is one of the largest concerns for consumers. For instance, a *Consumer Reports* poll revealed that "72 percent are concerned that their online behaviors were being tracked and profiled by companies" (Consumers-Union 2008).

To a great degree, these consumer worries are grounded in the growing "art of the possible" in the technological realm. The spread of ubiquitous computing and the seemingly unbounded options for collecting, processing, distributing, and using personal information trigger consumer worries. In a recent study analyzing the organizational privacy practices of the top 50 most visited websites, Gomez et al. (2009) found that most of these websites use personal information for customized advertising, and a large number of reputable firms like Google, Yahoo, Microsoft, and Facebook share their collected customer data with hundreds of their affiliated companies. Along with this use and sharing of data comes an associated risk: in the Ponemon Institute's 2007 survey with a sample of 786 American consumers, it was found that 62 percent of respondents had been notified that their confidential data was lost or stolen and that 84 percent of these consumers expressed increased concern or anxiety due to the data loss.

Against this backdrop, the number of privacy-related research contributions has grown significantly in recent decades. However, Information Systems (IS) researchers who wish to examine topics related to information privacy may well find themselves frustrated with the research domain. Numerous studies—a number of them based on compelling theoretical frameworks and undergirded by sound, rigorous, methodology—have been published over the past few decades. However, the findings and the theories that emerged have often relied on overlapping constructs nestled within loosely bounded nomological networks. This has resulted in a suboptimal cumulative contribution to knowledge.

In historical terms, it is now widely recognized that the recent evolution of the concept of privacy in general—and information privacy in particular—follows the evolution of information technology itself, as can be seen in Table 1.

While it is impossible for any discipline to claim ownership of the research concept of privacy in general, we believe that IS scholars' contributions to information privacy have been, and will continue to be, very important in shaping modernized information privacy conceptualization during the "third era."

In an attempt to assist the IS research community in providing a more cohesive treatment of information privacy issues, we first examine the privacy-related research that has been published to date. We consider the strengths and weaknesses of this research stream, and we then provide guidance regarding future directions for research. We rely on the following assumptions:

(1) The ultimate target of our review is *information* (rather than physical) privacy.

(2) Our target audience consists of IS scholars interested in empirical information privacy research.

(3) These scholars will be best enlightened by guidelines that are grounded in an interdisciplinary review of prior work.

(4) It is not our goal to build and propose a comprehensive, broad model of information privacy.

While we will provide some guidelines and outline the difficulties accompanying such an effort, it is well beyond the scope of our research endeavor to create such a meta-theory.

Literature Review

This literature review deals directly with information privacy as opposed to physical privacy. The latter concerns *physical* access to an individual and/or the individual's surroundings and private space; the former concerns access to individually identifiable personal *information*. Historically, the concept of physical privacy was explicated first. Later, as it became apparent that information about individuals and groups (especially families and organizational teams) was gathering saliency, information privacy was subsumed under the larger umbrella of general privacy.

In the initial period of this transition, physical privacy concepts and definitions were directly and seamlessly applied to information privacy, without reported contradictions. The continuity of the transition from physical privacy to information privacy allowed scholars to embrace the earlier adopted definitions and to carry them through specific contexts and cases associated with information privacy. More recently, however, nomological models associated with information privacy have been targeted directly to that construct. Thus, in a manner parallel to that of privacy research development, we will apply early privacy concepts to information privacy, and we will also analyze information privacy-specific concepts.

Table 1. Evolution of the Information Privacy Concept Following the Evolution of IT (adapted from Westin 2003)

Period	Characteristics
Privacy Baseline 1945-1960	Limited information technology developments, high public trust in government and business sector, and general comfort with the information collection.
First Era of Contemporary Privacy Development 1961-1979	Rise of information privacy as an explicit social, political, and legal issue. Early recognition of potential dark sides of the new technologies (Brenton 1964), formulation of the Fair Information Practices (FIP) Framework and establishing government regulatory mechanisms established such as the Privacy Act of 1974.
Second Era of Privacy Development 1980-1989	Rise of computer and network systems, database capabilities, federal legislation designed to channel the new technologies into FIP, including the Privacy Protection Act of 1984. European nations move to national data protection laws for both the private and public sectors
Third Era of Privacy Development 1990-present	Rise of the Internet, Web 2.0 and the terrorist attack of 9/11/2001 dramatically changed the landscape of information exchange. Reported privacy concerns rose to new highs.

We note that the distinction between physical and information privacy is seldom clarified in public debate or, for that matter, in many areas of research. For example, comments about *privacy violations* in the public media seldom draw a clear distinction between the constructs of physical and information privacy. Most of the questionnaires embraced in the cited literature ask about *privacy* rather than *information privacy*, as do the general surveys of polling agencies. In a related vein, popular terms and names of organizations, such as *privacy advocates*, *Privacy International*, *World Privacy Forum*, etc., are unclear in the distinction. The situation is the same with the legal language and the laws in many countries.

In an attempt to provide as direct a treatment of the concepts as possible, we will follow the following principle throughout the remainder of this paper: we will use the term *privacy* as a reference to *information privacy*, which is our immediate focus. We will occasionally refer specifically to *physical privacy* or to *general privacy* (which includes both physical and information privacy), and we intend those references to be distinct from those to (information) *privacy*.[2]

Although general privacy is broadly multidisciplinary in nature, each discipline offers a unique angle and perspective following its own accepted methodologies and discovery processes. Even so, across numerous disciplines, general privacy is often subsumed under the rubric of *ethics*. Indeed, in most encyclopedias, textbooks, and sociology readings (e.g., Bynum 2008; Pearlson and Saunders 2009), the topic of privacy is often found in the "ethical issues" chapter. As we will see below, general privacy beliefs are integrated in the moral value system of the society, and it is therefore natural that general privacy would be seen as an ethics topic. Consistent with this approach, we will classify general privacy studies using an ethics-based nomenclature of normative, purely descriptive, and empirically descriptive (Copp 2007; Singer 1991; Walsham 1996; Werhane 1994).

The word *normative* refers to guidelines or norms, so normative assertions rest upon ethical commitments and behaviors to be prized, preferred, and valued; they are often called *ought statements*. Examples of normative general ethical theories are Kantian ethics, virtue ethics, and utilitarian ethics. Examples of normative business ethics theories are stockholder, stakeholder, and social contract (Pearlson and Saunders 2009). In an overarching sense, *descriptive* studies attempt to explain what *is* rather than what ought to be. Descriptive studies can be *purely descriptive* (simple statements of fact) or *empirically descriptive* (tests of theories/frameworks utilizing positivist, scientific methods).[3]

[2]In many cases, we have had to rely on our own interpretations of other authors' covert assumptions about the distinctions as we classify and interpret their writings. Our heuristic is as follows: if a particular article/book (or group of articles/books) is clear in its orientation toward either physical or (information) privacy, we have categorized it as such. If the referent is either overtly stated as encompassing both domains, or if there is no statement but the author's covert assumptions appears (in our opinion) to encompass both, we have categorized it as general privacy.

[3]Although a particular study can be classified as primarily normative, purely descriptive, or empirically descriptive, the treatments do sometimes overlap, and in each a part of the other can sometimes be found (Werhane 1994).

Published studies can thus be classified as *normative*, *purely descriptive*, or *empirically descriptive.* The *normative* publications provide an ought argument for how the world should be, according to society's or the author's value system. Many (but not all) normative publications involve some statement of the author's opinion regarding an issue; per Herson (1990), some of these normative opinions may be buttressed by descriptive or empirical statements, but the overall tone of the argument is normative in its nature.

The *purely descriptive* studies are characterized by descriptions of a state of affairs, with no rigorous attempt to infer causality or to provide a process mapping. *Empirically descriptive* studies often attempt to provide tests of relationships between constructs or to map processes. For example, a study that tested a nomological model that showed how various psychological constructs such as cynicism and paranoia were associated with privacy concerns would be empirically descriptive.[4] Similarly, interpretive process tracing studies would also fall under the rubric of empirically descriptive studies.

In addition to their categorization as normative, purely descriptive, or empirically descriptive, general privacy studies can also be classified based on their *level of analysis*: individual, group, organizational, and societal (both cross-national and cross-cultural). In reviewing the literature by level of analysis, we follow the review methodologies embraced in previous scholarly work (Clark et al. 2007; Leidner and Kayworth 2006). Almost all empirical research associated with privacy has attempted to address one or more of these levels of analysis, but it will be seen that very little attention has been paid to group-level analysis.[5]

Appendix A describes the methodology used to identify general privacy publications. Tables B1, B2, and B3 provide summaries of the purely descriptive works, normative works, and empirically descriptive studies, respectively. Our analysis reveals that the works addressed to privacy have almost all been associated, in one way or another, with attempts to answer one of three major questions.

(1) *What is (and is not) privacy?* There is no single concept of privacy that crosses all disciplines and that is embraced by all observers. There are ongoing debates regarding the distinction, if any, between privacy and related constructs such as security.

(2) *What is the relationship between privacy and other constructs?* There are competing research assumptions and paradigms associated with empirical research into various nomological models that include privacy.

(3) *To what extent does context matter in the relationships between privacy and other constructs?* There is disagreement regarding the extent to which these relationships can be generalized across contexts, such as types of information, different industries, and new technological applications.

In the following sections, we discuss each of these major questions and provide a summary of the attempts to grapple with them. At the end of each section, we reflect on the work associated with that question. We summarize our reflections in our "Future Research and Conclusion" section.

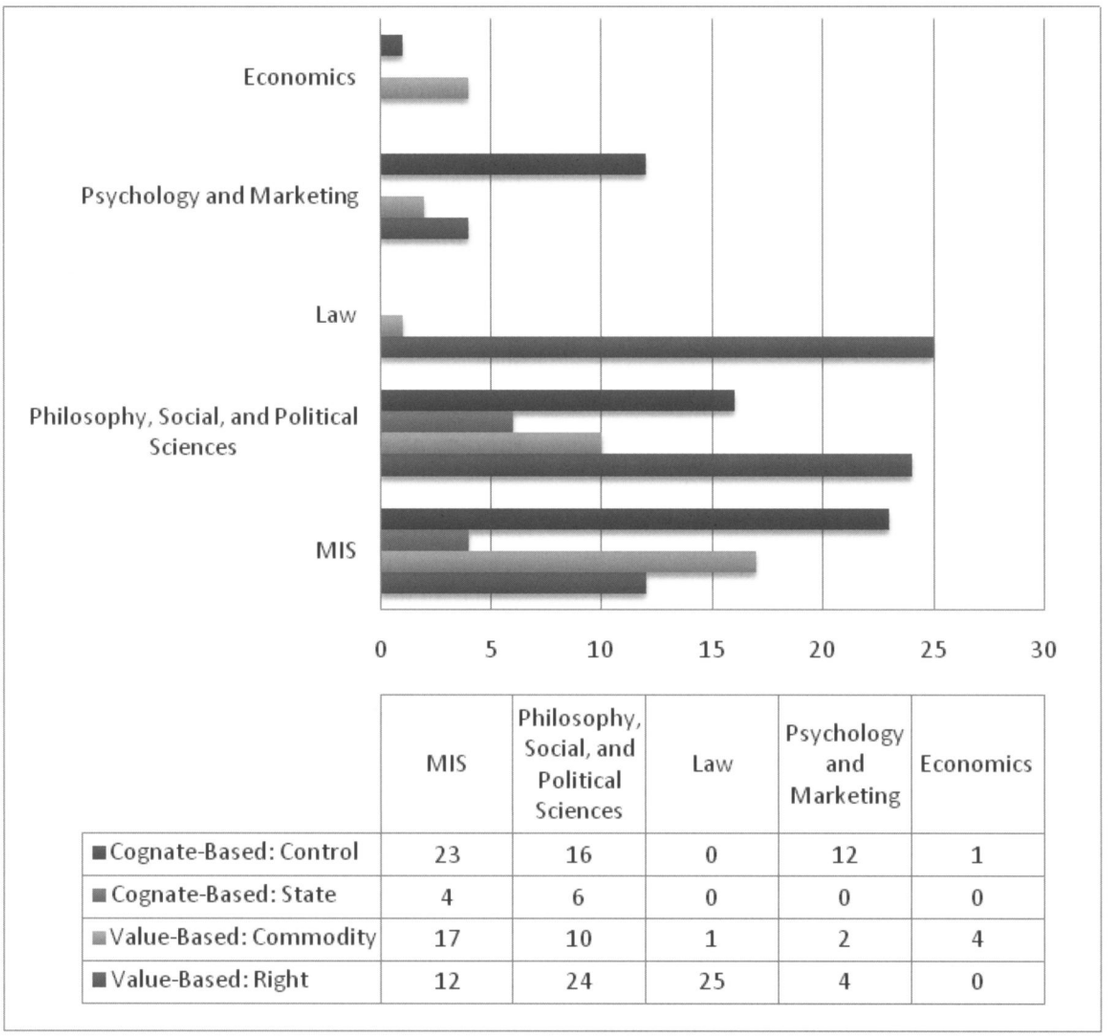
Question #1: What Is (and Is Not) Privacy?

General privacy as a philosophical, psychological, sociological, and legal concept has been researched for more than 100 years in almost all spheres of the social sciences. And yet, it is widely recognized that, as a concept, privacy "is in disarray [and n]obody can articulate what it means" (Solove 2006, p. 477). Numerous attempts have been made by social and legal scholars to bring together the different perspectives found in different fields. However, the picture that emerges is fragmented with concepts, definitions, and relationships that are inconsistent and neither fully developed nor empirically validated.

Figure 1 and Table B4 summarize the approaches to defining general privacy that can be found in various disciplines (corresponding to numbers of articles found in each discipline). The definitional approaches can be broadly classified as either *value-based* or *cognate-based.* The value-based definition views general privacy as a human right integral to society's

[4]Philosophers seldom distinguish between our categories of "purely descriptive" and "empirically descriptive" treatments. We note the distinction because it is important in IS and social science research.

[5]Although references to "groups" can be found in some IS analyses (e.g., Leidner and Kayworth 2006), a clear definition of a *group* (as opposed to an organization or a subunit) is seldom included. We embrace the view suggested by Propp and Kreps (1994) that members of a group are (1) pursuing interdependent goals, (2) have the ability to be aware of and react to each other, and (3) perceive themselves collectively to be a group. The specific size of such a group is subject to debate, although "traditionally, the majority of research on groups has focused on small groups of three to seven members" (Propp and Kreps 1994, p. 10). As will be discussed later, a clarification of definitional boundaries regarding groups should be a component of future research into online groups.



	MIS	Philosophy, Social, and Political Sciences	Law	Psychology and Marketing	Economics
Cognate-Based: Control	23	16	0	12	1
Cognate-Based: State	4	6	0	0	0
Value-Based: Commodity	17	10	1	2	4
Value-Based: Right	12	24	25	4	0

Figure 1. Approaches to Defining General Privacy (Refer to Table B4 for more details)

moral value system. Historically, this was the first definition of general privacy. Subsequent works defined the boundaries between public and private. The evolution of IT complicated the debate about the boundaries—a process seen by some scholars as *pervasive dissolution of the boundary* (Marx 2001; Rosen 2000) and by others as lack of rigor in defining these boundaries in the first place (Nissenbaum 1998).

Furthermore, when the *general privacy as right* concept was applied to consumer behavior, a *privacy paradox* was noted: despite reported high privacy concerns, consumers still readily submit their personal information in a number of circumstances. Thus, the notion of *privacy as a commodity* was conceptualized (Bennett 1995). Under the commodity view, privacy is still an individual and societal value, but it is not absolute, as it can be assigned an economic value and be considered in a cost–benefit calculation at both individual and societal levels.

In his attempt to supply a more rigorous definition that can be used in empirical research, Westin (1967) introduced the notion of *state* in the general privacy concept: "voluntary and temporary withdrawal of a person from the general society" (p. 7). Psychologists and cognitive scientists then became interested in producing a *cognate-based* conceptualization of general privacy–related to the individual's mind, perceptions,

and cognition rather than to an absolute moral value or norm. Since the state of withdrawal rests within the physical or information space, scholars argued that general privacy was about control of physical space and information. We now discuss the major definitional streams from each category in more detail.

Value-Based Definitions

General Privacy as a Right

There is a substantive debate regarding general privacy's status as a human right: If such a right exists, how did it emerge? How is it justified philosophically (Schoeman 1984)? Who is responsible for protecting it (Milberg et al (2000)? This view of general privacy is fundamentally normative, and some scholars (e.g., Posner 1984) claim that it may be at odds with the legal and societal frameworks of various cultures and thus cannot be treated absolutely.

The evolution of this debate is obvious when one considers the roots of general privacy as a right in legal and political theories. For example, in the United States, common law did not recognize any right to general privacy, general privacy is not spelled out in the U.S. Constitution, and the courts did not consider general privacy as a protected right until the 20th century. Although divergent from the traditional British perspective (Richards and Solove 2007), general privacy has generally been viewed as a developing right in U.S. law, with the U.S. derivation usually traced to Warren and Brandeis's (1890) article in *Harvard Law Review,* in which they defined general privacy as "the right to be left alone." This "general privacy as a right" perspective has since influenced numerous opinions and has been given constitutional sanction by the U.S. Supreme Court (Breckenridge 1970). Common themes of relevant court cases include general privacy and law enforcement (searches and seizures); general privacy and self (abortions and embryos); privacy and the press (private facts exposure, celebrity culture, intrusion); privacy and the voyeur (sex tapes, peephole); and privacy in the workplace (psychological testing, lifestyle monitoring) (Alderman and Kennedy 1997).

Two major issues arose with these court cases: 1) the need to define general privacy more specifically than the "right to be left alone" and (2) the state as the protector of general privacy. These two issues made the general privacy debate among legal and political scholars necessarily and unavoidably ideological. Regarding the first issue, courts have stopped seeking a definition of general privacy following the Younger Committee Report (1972), which concluded that general privacy could not be satisfactorily defined.

Regarding the second issue, two major camps of scholars argue about the role of the state in protecting individual general privacy and thus argue for or against the need for regulation of general privacy. The rallying point in the "for" argument among political theorists is the role of the state as the guarantor of individual general privacy (Rosen 2000). Ironically, the same principles of liberalism that undergird this argument also serve as the rallying point of the "against" libertarian camp of privacy protection. The against camp points to the market-based economic perspective of privacy. According to this view (to which we now turn), privacy is inherently an economic commodity and should be treated as such.

Privacy as a Commodity

Some libertarian political scientists argue that a call for greater privacy is, fundamentally, antagonistic to the political economy of the information markets (Bennett 1995; Cohen 2001). In their view, privacy is not an absolute right but is subject to the economic principles of cost–benefit analysis and trade-off. From this observation, a stream of treatment from the privacy as commodity perspective has arisen (Campbell and Carlson 2002; Davies 1997).

To explain the phenomenon of voluntarily providing information online (so-called *self-surveillance*) social scientists recognize the economic component of privacy: individuals cooperate in the online gathering of data about themselves as economic subjects. This participation in surveillance is possible because of recent reconceptualization of privacy in the consumer's mind from a right or civil liberty to a commodity that can be exchanged for perceived benefits (Campbell and Carlson 2002; Davies 1997; Garfinkel 2000).

Since libertarians have always treated privacy as a commodity, the salient question revolves around the extent to which the above observed commodification of privacy is a measurable result of a real individual shift and not a paradigm of scholarly shift. For example, Laudon (1996) has argued that the current crisis in the privacy of personal information is a result of market failure and calls for market correction through information technologies with privacy-enhancing mechanisms.

The distinction between privacy as a *right* and a *commodity*, although obviously undergirded by normative, value-laden assumptions, becomes important in empirical research. As will be seen in a later section in which we discuss the relationship between privacy and other constructs, many researchers unconsciously embrace one definition or the other without noting the value-laden assumptions.

Cognate-Based Definitions

General Privacy as a State

The *general privacy as a state* concept was introduced by Westin (1967), who defined privacy through four distinct substates: anonymity, solitude, reserve, and intimacy. Later, Schoeman (1984, p. 3) defined general privacy as "a state of limited access to a person." Weinstein (1971, p. 626) defined general privacy as a state of "being apart from others." He drew a parallel between general privacy and alienation, loneliness, ostracism, and isolation and noted that, among those, only general privacy is sought after whereas the others are avoided by individuals and are regarded by society as punitive. Further, Laufer and Wolfe (1977) conceptualized general privacy as a situational concept (state) tied to concrete situations with three dimensions: self-ego, environmental, and interpersonal. Information systems, economics, and marketing scholars narrowed these definitions of general privacy so that they addressed information-based issues (see Table B4). The *state of limited access* was translated to *state of limited access to information*.

When privacy is viewed as a state, it is natural for researchers to consider it in terms of its role as a sought-after goal (i.e., an individual's desire to exist in a state of privacy). The implication is that there must be a continuum of states of privacy, from absolute to minimal.

General Privacy as Control

The concept of general privacy as control originated in Westin's (1967) and Altman's (1975) theories of general privacy. Altman's definition of general privacy is "the selective control of access to the self" (p. 24). Margulis (1977a, 1977b) unified and elaborated on Westin's and Altman's perspectives and proposed a control-centered general privacy definition: "Privacy, as a whole or in part, 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" (1977a, p. 10). The control-based definition has since entered the mainstream of privacy research—likely because it lends itself more readily to the attributes of information privacy—and has been further developed in the fields of information systems and marketing (Altman 1975; Culnan 1993; Kelvin 1973; Margulis 1977a; Smith et al. 1996; Westin 1967). It is worth noting that the original definition equates privacy with control, *per se*, while most evolving definitions equate privacy with *ability* to control.

More frequently than not, the element of control is embedded in most conceptual arguments and definitions of privacy and has been used to operationalize privacy in numerous measurement instruments (Altman 1975; Culnan 1993; Kelvin 1973; Margulis 1977a; Smith et al. 1996; Westin 1967). Scholars have linked the concept of general privacy with control by either defining general privacy as control, *per se*, or by positioning control as a key factor shaping privacy. Johnson (1974), for instance, defined general privacy as "secondary control in the service of need-satisfying outcome effectance" (p. 91).

However, many researchers from several disciplines, including information systems, reason that control is actually one of the factors that shape general privacy and that general privacy is not control *per se* (Laufer and Wolfe 1977; Margulis 2003a, 2003b). For instance, Laufer and Wolfe (1977) conceptualized control as a mediating variable in the general privacy system by arguing that "a situation is not necessarily a [general] privacy situation simply because the individual perceives, experiences, or exercises control" (p. 26). Conversely, the individual may not perceive (s)he has control, yet the environmental and interpersonal elements may create perceptions of general privacy (Laufer and Wolfe 1977). As Margulis (2003a, 2003b) pointed out, there have been very few theoretical attempts to clarify the nature of control and to explicate this control: privacy contention in the privacy literature (exceptions are Dinev and Hart 2004; Johnson 1974; Xu 2007).[6]

What Privacy Is Not

Privacy has been described as multidimensional, elastic, and dynamic in the sense that it varies with life experience (Altman 1977; Laufer and Wolfe 1977). Overlapping concepts such as confidentiality, secrecy, anonymity, security, and ethics have added to the confusion (Margulis 2003a, 2003b). Therefore, Question #1 also asks what privacy is *not*. Although there is confusion regarding the boundaries around the construct, much of the murkiness can be stripped away by a careful consideration of the distinctions.

[6]Privacy is frequently defined in IS and many branches of social science research in phrases such as "the ability of individuals to control the terms under which their personal information is acquired and used" (Culnan and Bies 2003, p. 326), which is adapted from Westin's (1967) definition. Such a definition is nonnormative, because it assumes no right to privacy, and it also implies no specific tradeoff with other commodities. This definition does not rely on any assumptions about a state of being, which reduces the ambiguity inherent in empirical assessment thereof. This definition may be less useful for philosophical discourse, although such discourse is seldom associated with empirical research.

Anonymity: Anonymity is the ability to conceal a person's identity (Camp 1999; Marx 1999; Qian and Scott 2007; Rensel et al. 2006; Zwick and Dholakia 2004), which is central for the information collected for statistical purposes. In the IT context, anonymity is often shaped by the features of privacy-enhancing technologies. For example, anonymizers allow an individual to browse Web sites with a high degree of anonymity, as cookies cannot be placed on the user's browser and the IP addresses cannot be tracked (Waldo et al. 2007). Anonymity is not dichotomous, in that it varies in degrees (Kobsa and Schreck 2003; Nissenbaum 1999; Qian and Scott 2007): individuals can choose to be totally anonymous, pseudonymous, or identifiable.

There has been much discussion as to what role anonymity plays in privacy. Although these two concepts interrelate, *anonymity is not privacy* (Camp 1999). Anonymity exists when someone is acting in a way that limits the availability of identifiers to others. Since the information cannot be correlated back to the individual, this may enable privacy control. However, many other avenues to such control also exist.

Secrecy: Secrecy has been defined as intentional concealment of information (Bok 1989; Tefft 1980), and it usually expresses a disposition toward the sharing of potentially inaccurate information (Zwick and Dholakia 2004). Secretive withholding of personal information is then regarded as an attempt to block any digital representation from emerging in the network. Although secrecy is easily distinguishable from privacy (Hirshleifer 1980), they are often mistaken and confused with each other (McLean 1995). "Privacy need not hide; and secrecy hides far more than what is private" (Bok 1989, p. 11). Warren and Laslett (1977) also reflect on the conceptual comparison between privacy and secrecy. According to them, secrecy implies the concealment of something that is negatively valued by the excluded audience; privacy, by contrast, protects behavior which is either morally neutral or valued by society. Secrecy enables individuals to manipulate and control environments by denying outsiders vital information about themselves (Tefft 1980).

Confidentiality: Richards and Solove (2007) suggest that while the American derivation of general privacy is grounded in one's inviolate personality (focus on individualism), British law instead embraces a conception of privacy as confidentiality. With the advent of extensive information exchange, confidentiality concerns the externalization of restricted but accurate information to a specific entity (Zwick and Dholakia 2004). The distinction between privacy and confidentiality is well discussed in the literature (Camp 1999; Rindfleisch 1997). Privacy corresponds to the desire of a person to control the disclosure of personal information; confidentiality corresponds to the controlled release of personal information to an information custodian under an agreement that limits the extent and conditions under which that information may be used or released further.

Building on Zwick and Dholakia's (2004) conceptualization of identity management, we can differentiate anonymity, secrecy, and confidentiality based on the externalization of personal information. Figure 2 illustrates how the various constructs are related based on the digital representation of an individual, which is determined by the *amount* and *accuracy* of the personal information collected. Of course, none of the constructs in Figure 2 is equivalent to privacy itself.

Security: The perceptions or concerns of security by users of electronic systems has been addressed in IS research (Benson 1983; Goodhue and Straub 1991; White and Christy 1987) but, as has been pointed out by Belanger et al. (2002), there is a lack of understanding of how privacy and security issues are related. Security corresponds to the concerns about the protection of personal information with three specific goals (Belanger et al. 2002; Camp 1999; Chellappa 2008): integrity that assures information is not altered during transit and storage; authentication that addresses the verification of a user's identity and eligibility to data access; and confidentiality that requires data use is confined to authorized purposes by authorized people. As Culnan and Williams (2009) argue, organizations can successfully secure the stored personal information but still make bad decisions about the subsequent use of personal information, resulting in information privacy problems. Therefore, as Ackerman (2004) suggested, "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).

Ethics : As mentioned above, general privacy has consistently been viewed as an ethical issue across various disciplines. While there are ethical dimensions associated with general privacy (Ashworth and Free 2006; Caudill and Murphy 2000; Culnan and Williams 2009; Foxman and Kilcoyne 1993), general privacy is not equivalent to ethics. General privacy has been examined in the literature from a number of ethical theoretical perspectives including social contract theory, duty-based theory, stakeholder theory, virtue ethics theory, and the power–responsibility equilibrium model (for a review, see Caudill and Murphy 2000). Even though philosophical argumentation may imply some normative ethical obligations to protect or to acknowledge privacy, it is incorrect to equate privacy with ethics. In fact, one can easily engage in empirical privacy-related research without ever considering ethical aspects of the construct.

In that light, having now considered what privacy is (and is not), we turn to a consideration of its empirical treatment across various disciplines.

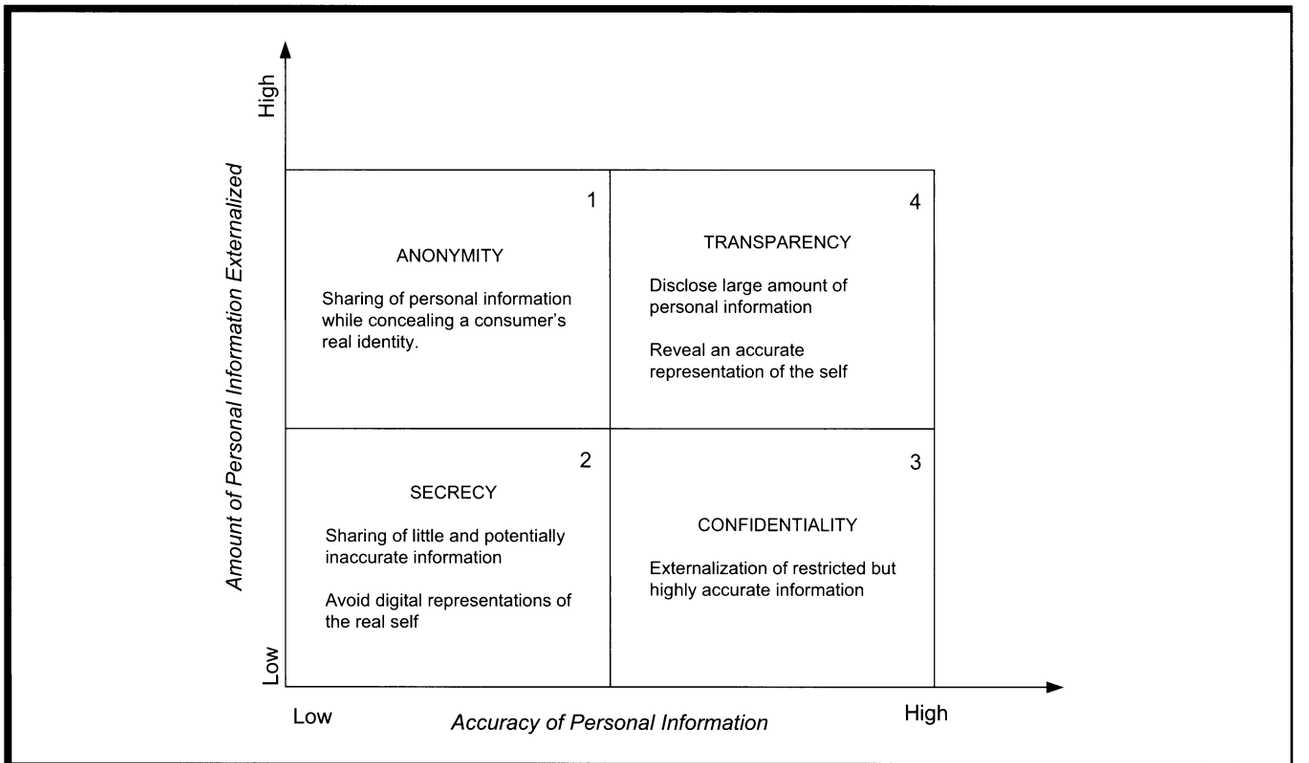


Figure 2. Tactics of Identity Management (Adapted from Zwick and Dholakia 2004)

Question #2: What Is the Relationship Between Privacy and Other Constructs? ■

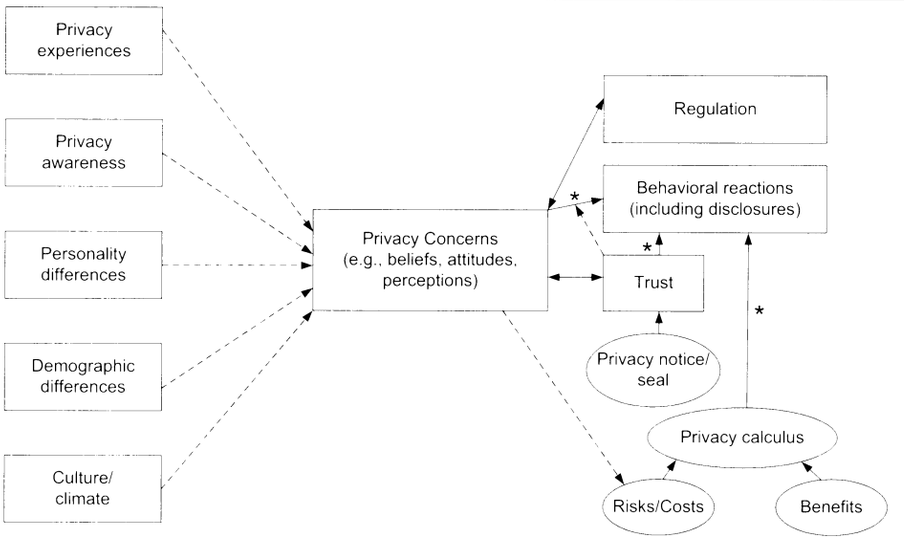
The relationship between privacy and other constructs has been examined by a number of empirically descriptive (and primarily positivist) studies that cut across several disciplines such as marketing, IS, and organizational behavior (see Figure 3).

We first examine the central construct in this figure ("Privacy Concerns"); we then consider the antecedents (on the left), and we then focus on the outcomes and associated relationships (on the right). We refer to this macro model as "Antecedents → Privacy Concerns → Outcomes" (APCO).

Privacy Concerns as a Measurable Proxy for Privacy

Because of the near impossibility of measuring privacy itself, and also because the salient relationships depend more on cognitions and perceptions than on rational assessments, almost all empirical privacy research in the social sciences relies on measurement of a privacy-related proxy of some sort. Although the proxies sometimes travel with monikers such as *beliefs*, *attitudes*, and *perceptions*, over time, especially within IS research, there has been a movement toward the measurement of *privacy concerns* as the central construct. Several studies have operationalized privacy concerns in detail: The concern for information privacy (CFIP) scale was developed by Smith et al. (1996), who identified four data-related dimensions of privacy concerns (collection, errors, secondary use, and unauthorized access to information). These dimensions were later revalidated by Stewart and Segars (2002). These dimensions have since served as some of the most reliable scales for measuring individuals' concerns toward organizational privacy practices. More recently, Malhotra et al. (2004) operationalized a multidimensional scale of Internet users' information privacy concerns (IUIPC), which adapted the CFIP into the Internet context.

It should be noted that these privacy concerns are almost always measured at an *individual* level of analysis, so most of the research on the left side of Figure 3 has an individual unit as its dependent variable (DV). However, not all of the inde-



Dotted lines indicate that the relationship is tenuous (i.e., has not been confirmed through repeated studies).

Not shown: Possible two-way loop, in which some actions on the right may impact some constructs on the left.

*Results threatened by privacy paradox, since usually intentions (not behaviors) have been measured.

Figure 3. Relationships Between Privacy and Other Constructs: Antecedents → Privacy Concerns → Outcomes (APCO Macro Model)

pendent variables (IVs) are measured at the individual level, as some (e.g., culture/climate) are at the organizational or national level.

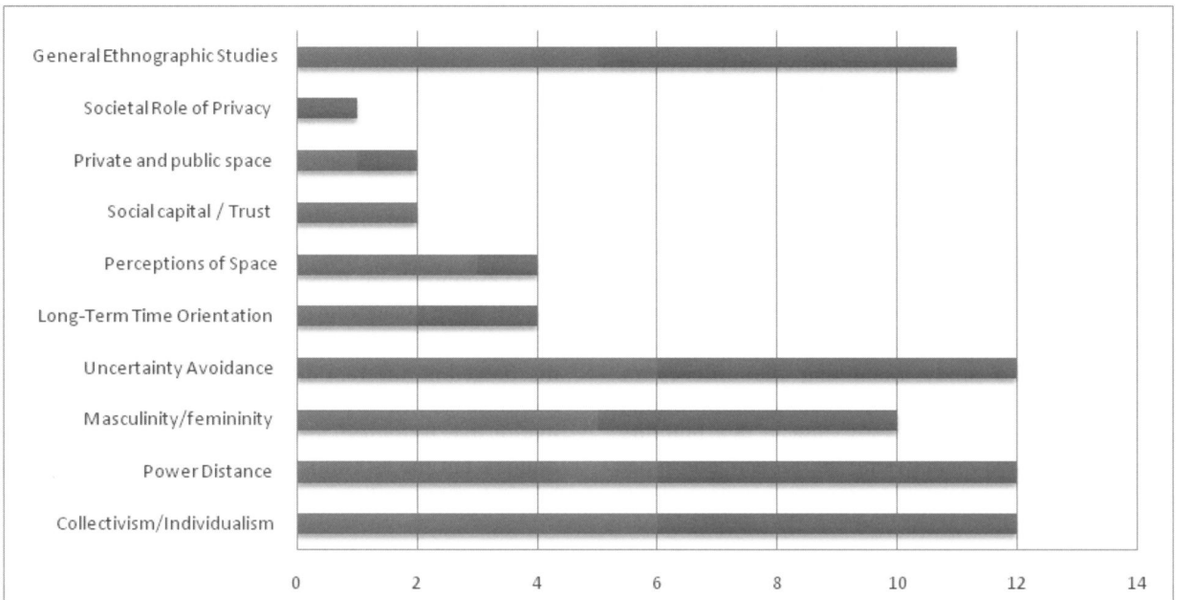
Privacy Concerns as Dependent Variable (DV)

Although relationships between a number of antecedents and privacy concerns have been investigated, these studies have usually been conducted in a somewhat disjointed manner and with only minimal replication. A smaller body of research has systematically emerged on the left-hand side of Figure 3. Drawing on information boundary theory, Xu et al. (2008) developed an integrative model suggesting that privacy concerns form because of an individual's personal characteristics or situational cues that enable one person to assess the consequences of information disclosure.

With respect to *privacy experiences*, Smith et al. (1996) found that individuals who have been exposed to or been the victim of personal information abuses should have stronger concerns regarding information privacy. *Privacy awareness* reflects the extent to which an individual is informed about organizational privacy practices (Malhotra et al. 2004; Phelps et al. 2000). Research suggests that consumers' privacy concerns are triggered when consumers become aware that organizations have collected and/or used their personal information without their permission (Cespedes and Smith 1993). Consumers who are unaware of name removal procedures tend to be less likely to be concerned about privacy than consumers who are aware of name removal procedures (Culnan 1995). It has been found that consumers tend to be less concerned about their privacy when firms seek permission to collect and use their information (Nowak and Phelps 1995).

Personality differences such as introversion versus extroversion (Lu et al. 2004), independent-self versus interdependent-self (Xu 2007), and "big-five" personality traits[7] (Bansal et al. 2010) have been found to affect individual privacy concerns. Dinev and Hart (2006) found that social awareness is a predictor of privacy concerns. Individuals with high social awareness are aware of privacy policies and follow privacy issue developments. Various studies have also investigated how *demographic differences*

[7]Bansal et al. (2010) examined the role of the "big five" personality traits in influencing individuals' perceptions of health information sensitivity. These five dimensions of personality are extroversion, agreeableness, emotional instability, conscientiousness, and intellect.



	Collectivism /Individualism	Power Distance	Masculinity /femininity	Uncertainty Avoidance	Long-Term Time Orientation	Perceptions of Space	Social capital / Trust	Private and public space	Societal Role of Privacy	General Ethnographic Studies
Individual level	6	6	5	6	2	3	2	1	0	4
Group level	0	0	0	0	0	0	0	0	0	1
Organizational level	0	0	0	0	0	0	0	0	0	0
Societal/cultural/international level	6	6	5	6	2	1	0	1	1	6

Figure 4. Studies Related to Cross-Cultural Contexts (Refer to Table B5 for more details)

affect the degree of stated privacy concerns (Chen and Rea 2004; Culnan and Armstrong 1999; Sheehan 1999; Sheehan and Hoy 2000). For example, women have been found to be generally more concerned than men about the impact of information collection on their privacy (Sheehan 1999). Also, it was found that those consumers who were less likely to be concerned about privacy were more likely to be young, poor, less educated, and African-American (Culnan 1995).

Cross-cultural antecedents have also been considered as independent variables (see Figure 4 and Table B), most often at the individual and the societal levels. For example, Dinev et al (2006a, 2006b) showed that Italian society has a different concept of privacy that leads to lower privacy concerns but also to higher perceived risk. These differences inform weaker relationships between institutional trust and e-commerce use, privacy concerns and e-commerce use, and perceived risk and institutional trust, and a stronger relationship between perceived risk and privacy concerns.

Privacy Concerns as Independent Variable (IV)

In contrast to the limited empirical attention that has been focused on relationships between antecedents and privacy concerns, a larger body of research has emerged on the right-hand side of APCO model in Figure 3: that is, consideration of privacy concerns as an IV in which other outcomes are viewed as the DVs.

Behavioral reactions. The most prominent DVs are those associated with behavioral reactions to privacy concerns, with the most visible reactions being individuals' willingness to disclose information and/or to engage in commerce. Some researchers have viewed *trust* as a mediating variable between privacy concerns and disclosure itself (Metzger 2004; Xu et al. 2005), but in many other studies trust has been shown to be antecedent to privacy (e.g., Belanger et al. 2002), outcome of

privacy (e.g., Bansal et al. 2010; Chellappa 2008; Malhotra et al. 2004), or a moderator/mitigator (e.g., Bansal et al. 2008) of the influence of privacy concerns on individual behavioral reactions. In one study of 477 U.S. households, researchers found that privacy concerns had a significant impact on online purchase intent, with the greatest negative impact being through its relationship with trust (Eastlick et al. 2006). Firms that are positioned as "safer" or "trustworthy" on the privacy dimension will likely have a competitive advantage (Bowie and Jamal 2006). It has been found that consumers who trust the firm are less concerned about their privacy and more willing to provide personal information (Schoenbachler and Gordon 2002). In a study examining the efficacy of improving trust and reducing concern on managing consumer information, Milne and Boza (1999) showed that building trust is more effective than trying to reduce consumer concern.

Research has found that firms can build trust, and thus mitigate privacy fears, by exhibiting procedural justice through the implementation of fair information practices (Culnan and Armstrong 1999; Xu et al. 2010), explicit communication of a privacy policy (Andrade et al. 2002; Eastlick et al. 2006; Milne and Boza 1999), adoption of P3P in their privacy policy development (Xu et al. 2005), and/or display of privacy notices and/or seals of approval (LaRose and Rifon 2006; Wang et al. 2004). The presence of privacy seals has been found to have a positive effect on the perception of trust in a website (Rifon et al. 2005) and resulted in more favorable perceptions toward the privacy statement (Miyazaki and Krishnamurthy 2002).[8]

Privacy paradox. Recent surveys, anecdotal evidence, and experiments have highlighted the privacy paradox: individuals state privacy concerns but behave in ways that seemingly contradict their statements (Acquisti 2004; Acquisti and Grossklags 2005a; Jensen et al. 2005; Norberg et al. 2007). For example, Sheehan and Hoy (1999) found that stated privacy concern correlates negatively with the reported frequency of registering with websites in the past and positively with providing incomplete information during registration. Norberg et al. (2007) found that, for all information categories (personally identifying, financial, preferences, demographic, etc.), the level of actual disclosure significantly exceeded individuals' intentions to disclose information.

A plausible explanation provided by Acquisti's work for such a privacy attitude/behavior dichotomy is that users' privacy decision processes are affected by bounded rationality (Acquisti 2004; Acquisti and Grossklags 2005b). The economics literature suggests that individuals have a tendency to discount "hyperbolically" future costs or benefits (O'Donoghue and Rabin 2001; Rabin and O'Donoghue 2000). Such hyperbolic discounting implies inconsistency of personal preference over time: future events may be discounted at different discount rates than near-term events (Acquisti 2004); the benefits of disclosing personal information may be immediate (e.g., convenience of placing orders online), but the risk of such information disclosure may be invisible or spread over time (e.g., identity theft).

Although Figure 3 includes the construct "behavioral reactions" on its right-hand side, in reality it is quite common for researchers to measure stated *intentions* instead of actual behaviors, inferring through references to the theory of reasoned action (TRA) (Fishbein and Ajzen 1975), that behaviors will match actual intentions. To the extent that the privacy paradox holds, however, this appeal to TRA may be misguided. In fact, associations between privacy concerns and stated intentions may not be reflective of actual behaviors. We have noted this exposure in Figure 3 with asterisks.

Regulation. In addition to behavioral reactions associated with disclosure and commerce, Milberg et al. (2000) suggest that if consumers do not perceive firms as adequately protecting their privacy, they will distrust self-regulation and prefer state intervention, which can eventually lead to a regulatory response. A limited stream of research (see, especially, Jentzsch 2001; Smith 2001) has investigated the dissonance between U.S. and European privacy laws, which is related to the conflict between viewing privacy as a *right* versus a *commodity*. Jentzsch (2001) has noted that Europe assigns more property rights to consumers than does the United States, and financial privacy is more strictly regulated in Europe than in the U.S., although the U.S. seems to be converging more on the European model.

At the societal level, several studies pointed out that human rights societies long approached privacy in an omnibus fashion by passing sweeping privacy bills that address all the instances of data collection, use, and sharing (Bennett and Raab 1997; Dholakia and Zwick 2001; Smith 2001). Some examples of countries in this category include Australia, Canada, New Zealand, and countries in the European Union

[8]However, a number of recent studies uncovered weak consumer trust toward third-party certification agencies. Several studies came to the conclusion that websites that decide to "pay up" for certain privacy seals seem to have more questionable privacy practices than ones that do not (Edelman 2011). LaRose and Rifon (2006) found that sealed sites requested significantly more personal information from users than unsealed sites. Miyazaki and Krishnamurthy (2002) reviewed 60 high-traffic websites and found no support for the hypothesis that participation in a seal program is an indicator of better privacy practices (LaRose and Rifon made similar findings).

(Smith 2004). Assigning fundamental rights to personal information would result largely in an opt-in market for information sharing, whereby firms would have access to the information only of those consumers who chose to make it available (Smith 2001). In contrast, in commodity societies, there are no omnibus laws governing collection, use, and sharing of personal information that transcend all types of data in all sectors of the economy (Smith 2001). Some countries in this category have a patchwork of sector-specific privacy laws that apply to certain forms of data or specific industry sectors (Bennett and Raab 1997; Dholakia and Zwick 2001; Smith 2001). For instance, in the United States, there are sector-specific laws for specific types of records such as credit reports and video rental records and for classes of sensitive information such as health information (Smith 2004). The commodity societies largely see opt-in as an undue burden.

The debate between the right and commodity views of privacy highlights another controversial issue in the privacy literature: the relative effectiveness of industry self-regulation versus government legislation in ensuring consumer privacy. Skepticism about the effectiveness of industry self-regulation in protecting consumer privacy (Edelman 2011; Hui et al. 2007) has resulted in privacy advocates and consumers clamoring for strong and effective legislation to curtail rampant abuses of information by firms. At the societal level, Tang et al. (2008) indicate that although overarching government regulations can enhance consumer trust, regulation may not be socially optimal in all environments because of lower profit margins for firms and higher prices for consumers. Bellman et al. (2004) found that participants from countries with omnibus privacy regulation had greater desire for more regulation than participants from countries with sectoral regulation, while participants from countries with sectoral privacy regulation had less desire for more regulation than participants from countries with no privacy regulation.

Privacy Calculus

A subset of empirical studies—often somewhat disconnected from the other constructs within Figure 3—addresses the concept of *privacy calculus* by assuming that a consequentialist tradeoff of costs and benefits is salient in determining an individual's behavioral reactions. This perspective is found in various works (e.g., Klopfer and Rubenstein 1977; Laufer and Wolfe 1977; Posner 1981; Stone and Stone 1990) that view the concept of privacy as not absolute but, rather, subject to interpretation in "economic terms" (Klopfer and Rubenstein 1977, p. 64). Such a calculus perspective of privacy suggests that, when requested to provide personal information to corporations, consumers would perform a risk–benefit analysis to assess the outcomes they would face in return for the information, and respond accordingly (Chellappa and Sin 2005; Culnan 1993; Dinev and Hart 2006; Hann et al. 2008; Hui et al. 2006; Milne and Gordon 1993; Milne and Rohm 2000; Xu et al. 2010). We consider these risks and benefits.

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 (Featherman and Pavlou 2003; Malhotra et al. 2004). In the privacy literature, although privacy concerns have often been treated as a multidimensional construct (Malhotra et al. 2004; Smith et al. 1996), *privacy risk* has been treated as a single-dimensional construct that measures potential loss of control over personal information (e.g., Dinev and Hart 2006). Prior privacy literature has identified sources of organizational opportunistic behavior, including insider disclosure or unauthorized access and theft (Rindfleisch 1997), and selling personal data to, or sharing information with, third parties, financial institutions (Budnitz 1998), or government agencies (Preston 2004; Wald 2004). An individual's calculation of risk involves an assessment of the likelihood of negative consequences as well as the perceived severity of those consequences (Peter and Tarpey 1975). The negative perceptions related to risk may affect an individual emotionally, materially, and physically (Moon 2000). A number of e-commerce studies empirically verified the negative effect of perceived risk on intentions to conduct transactions (Budnitz 1998; Jarvenpaa and Leidner 1999; Jarvenpaa and Tiller 1999; Jarvenpaa et al. 2000; Norberg and Horne 2007; Norberg et al. 2007; Pavlou 2003; Pavlou and Gefen 2004). Additionally, previous studies generally supported the positive impacts of privacy risk on privacy concerns (Dinev et al. 2006b; Dinev and Hart 2004), and the negative impacts of privacy risk on intention to disclose personal information (Malhotra et al. 2004; Xu et al. 2005).

Privacy benefit. Following the notion of privacy calculus, "individuals are assumed to behave in ways that they believe will result in the most favorable net level of outcomes" (Stone and Stone 1990, p. 363). Scholars have identified three major components of benefits of information disclosure including financial rewards, personalization, and social adjustment benefits. Recent privacy studies provide empirical evidence that compensating consumers through financial rewards can foster their information disclosure (Caudill and Murphy 2000; Hann et al. 2008; Phelps et al. 2000; Xu et al. 2010). In terms of the value of personalization, Chellappa and Sin (2005) found that it can override privacy concerns: "the consumers' value for personalization is almost two times…more influential than the consumers' concerns for privacy in deter-

mining usage of personalization services" (p. 197). A study by White (2004) also confirmed that users are more likely to provide personal information when they receive personalization benefits. A study by Lu et al. (2004) demonstrated that social adjustment benefits (defined as the establishment of social identity by integrating into desired social groups) can also have an effect on intended disclosure behavior.

Looking Across the Empirical Research

In looking across the empirically descriptive (and primarily positivist) privacy research to date, it can be observed that the unit of analysis varies little within these studies; in particular, most studies from the privacy as a commodity perspective (including privacy calculus and privacy paradox) have considered only the individual unit of analysis (with Dinev et al. (2006b) an exception that addressed the societal level of analysis). No studies have considered the *group* level of analysis, and only a very few (represented in the sample by Walczuch and Steeghs 2001) have addressed the organizational unit of analysis in the context of these perspectives.

It will also be recalled, from our earlier discussion of Figure 3, that research attention to the overall antecedents → privacy concerns → outcomes (APCO) rubric has been distributed non-uniformly. In particular, almost all of the research focus has been associated with the linkage between privacy concerns and outcomes (usually at the organizational or societal level), with very little attention having been paid to the linkage between antecedents and privacy concerns (and what has been attempted has usually been at the individual level of analysis). Further, the theoretical and empirical connections between the APCO rubric and the privacy calculus stream are rather muted, which causes frustration for observers who wish to view all of the research findings in a cohesive framework.

It is rather clear, then, that the empirical research stream has to date been somewhat constrained. And, as will be seen as we consider Question #3, the picture is even further muddied when we consider the matter of context.

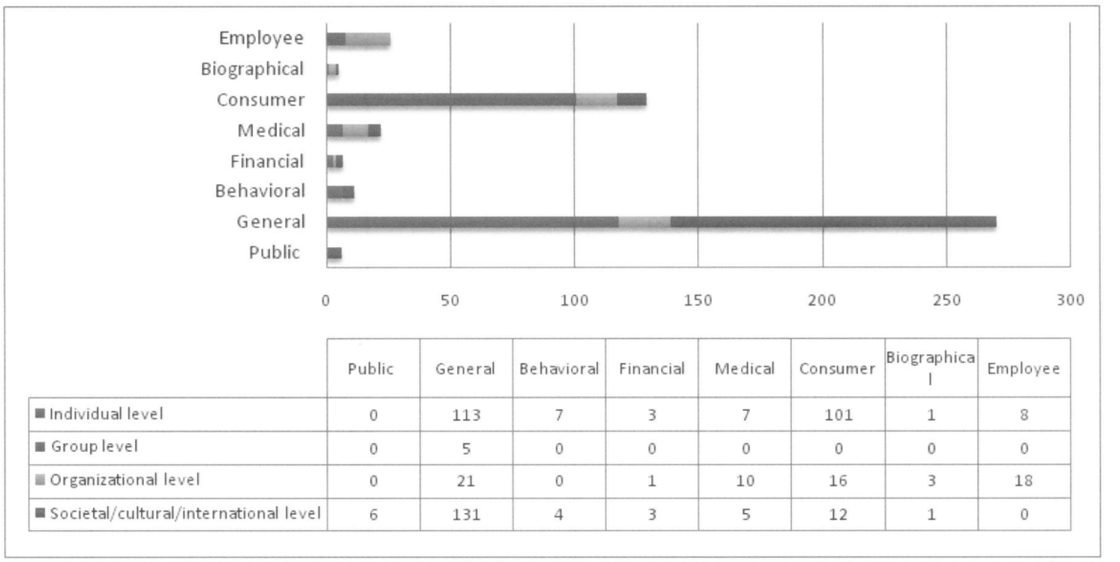
Question #3: To What Extent Does Context Matter in the Relationships between Privacy and Other Constructs?

Contextual Nature of Privacy

In our examination of Question #2, we proceeded as though privacy was a construct that could be considered as a singular entity. Yet, many legal and social scholars (Altman 1975, 1977; Hirshleifer 1980; Laufer and Wolfe 1977; Lederer et al. 2004; Malhotra et al. 2004; Margulis 1977a, 2003a; Solove 2004, 2006, 2008; Waldo et al. 2007; Westin 1967, 2001, 2003) believe that general privacy—its conceptual understanding, rigorous definition, and the intensity of the individual and cultural beliefs it informs—is so dependent on the specific context that it is impossible to develop a one-size-fits-all conceptualization of general privacy. Scholars have tended to conclude that it can mean different things to different individuals and, hence, the roots and consequences of its violation are also contextual (Bennett 1992).

Acquisti (2004) holds that privacy should be regarded more as a class of multifaceted interests than as a single, unambiguous concept, and its value may be discussed only once its context has also been specified. Recently, Bansal et al. (2008) provided a review of the general definitions and meaning of context. Context has been defined as "stimuli and phenomena that surround and, thus, exist in the environment external to the individual, most often at a different level of analysis" (Mowday and Sutton 1993, p. 198). Context could be related to the type or domain of the research construct (discipline), time (when), location (where), occupation (who), culture (with whom), and rationale (why) (Bansal et al. 2008). For example, the industry to which an organization belongs can be viewed as a contextual variable; longitudinal studies can be viewed as contextual studies with time as the contextual variable (when); comparisons of behavior and beliefs across occupation, gender, race, income, culture, etc. can be viewed as contextual studies, demographic being the contextual variables (who); comparing privacy concerns across different types of information or web sites with different levels of information exchange renders the "type of information" or "information sensitivity" (Malhotra et al. 2004) as contextual variables (see also Bansal et al. 2008).

Individuals are continually engaging in an adjustment process in which desires for privacy are weighed against desires for disclosure and personal communication with others (Kimmel 1996; Sheehan 2002). The adjustment occurs in the context of various situational forces, such as pressures from others, societal and political norms, and processes of surveillance used to enforce them (Kimmel 1996). Privacy either depends on or derives from the nature of its threats (Regan 1995; Sheehan 2002). Indeed, context has been found to moderate (Bellman et al. 2004; Dinev et al. 2006a, 2006b; Milberg et al. 1995; Smith et al. 1996) or to directly influence (Malhotra et al. 2004) the nature and extent of privacy-related relationships (see also Pedersen 1997, 1999).



	Public	General	Behavioral	Financial	Medical	Consumer	Biographical	Employee
Individual level	0	113	7	3	7	101	1	8
Group level	0	5	0	0	0	0	0	0
Organizational level	0	21	0	1	10	16	3	18
Societal/cultural/international level	6	131	4	3	5	12	1	0

Figure 5. Studies Based on Type of Information (Refer to Table B6 for more details)

In our analysis of the privacy research, we found that the most often cited contexts for privacy and privacy-related beliefs are (1) the type of information collected from individuals (e.g., behavioral, financial, medical, biometric, consumer, biographical); (2) the use of information by sector (e.g., healthcare, marketing, and finance); (3) political context (e.g. law enforcement, constitutional rights of self, government, pubic data and media); and (4) technological applications.

The first context, the types of information collected, is sometimes referred to as contextual sensitivity or information sensitivity (Malhotra et al. 2004): consumers' beliefs and behavioral responses to privacy threats depend on the type of information requested (Dinev and Hart 2007; Milne and Gordon 1993; Phelps et al. 2000; Sheehan and Hoy 2000). In general, information about lifestyle characteristics and shopping habits and preferences are considered less sensitive than medical and financial information (Nowak and Phelps 1992; Phelps et al. 2000; Sheehan and Hoy 2000). Malhotra et al. (2004) found a statistically significant direct effect of information sensitivity on trusting beliefs, risk beliefs, and behavioral intention. Xu et al. (2008) confirmed that privacy-related relationships do vary across types of web sites (e-commerce, social networking, financial, and healthcare), reflecting the information sensitivity context. Figure 5 and Table B6 summarize the studies based on the type of information collected, sorted by different levels of analysis. (Studies that do not consider a specific type of information often simply refer to phrases such as "information that most individuals would categorize as private." These studies are noted in the "general" category in Figure 5 and Table B6.)

The second context, industry sector, is considered in Table B7. For example, there are many IS studies that explore privacy in e-commerce, marketing, and healthcare. The third context, the political context of general privacy, is especially evident in the U.S. and European legal framework and constitutions. Many legal and social scholars view general privacy as a value that must be balanced against other values that individuals see as important, including the rights of self, freedom of the press, law and order, and national security (Etzioni 1999; Regan 1995). Most of the literature that examines general privacy issues in these political contexts is normative and sometimes emotionally charged, usually reflecting the authors' strong beliefs in their causes (see Table B8).

The fourth context, technological applications, complicates privacy research due to the potential duality of its relationships. On the one hand, it is often covertly assumed that new technological applications will lead to new concerns and outcomes; at the same time, privacy protections could be implemented through privacy-enhancing technological applications. Although some of the studies have overlapped with some of the studies discussed in Question #2, the majority of these investigations have proceeded on largely parallel lines that assume a new stream of research is warranted for each new technological

Table 2. Influences of Technological Attributes on Privacy Concerns

Technological Attributes	Individual Level	Group Level	Organizational Level	Societal Level
Direct Marketing	Blattberg and Deighton 1991; Campbell 1997; Culnan 1993, 1995; Milne 1997; Milne et al. 1999; Nowak and Phelps 1992, 1997; Sheehan and Hoy 1999; Smith et al. 1996			
Internet and e-commerce	Acquisti and Varian 2005; Dhillon and Moores 2001; Dinev and Hart 2004, 2006; Dolnicar and Jordaan 2007; Hoffman et al. 1999; Malhotra et al. 2004; Odlyzko 2004; Van Slyke et al. 2006; Taylor 2004a, 2004b		Bowie and Jamal 2006; Culnan 2000; Henderson 1999; McRobb and Rogerson 2004; Milne and Culnan 2002; Schwaig et al. 2006; Shah et al. 2007	Laudon 1996
Data Mining and Profiling (personalization)	Awad and Krishnan 2006; Chellappa and Sin 2005; Cranor 2003; Kobsa 2002, 2007			
Monitoring and Surveillance	Allen et al. 2007; Fairweather 1999; Tabak and Smith 2005; Zweig and Webster 2002; Zweig and Webster 2003		Ariss 2002; D'Urso 2006; Stone-Romero et al. 2003; Tabak and Smith 2005	Dinev et al. 2006a; Kim 2004
Communication (email, IM, and SMS)	Häkkilä and Chatfield 2005; Meeks 1997, 1999	Grinter and Palen 2002; Ito and Daisuke 2003; Ling 2004; Shapiro 1998	Sipior and Ward 1995; Sipior et al. 1998; Weisband and Reinig 1995	
Ubiquitous Computing (Mobile and Location-Enhanced Technologies and RFID)	Bruner and Kumar 2007; Junglas and Spitzmüller 2005; Lederer et al. 2003; McGinity 2000; Sheng et al. 2008; Unni and Harmon 2007; Xu and Gupta 2009; Xu and Teo 2004; Xu et al. 2010			Clarke 2001
Web 2.0 (Online Social Networks)	Acquisti and Gross 2006; Boyd 2008; Boyd and Ellison 2007; Dinev et al. 2009; Dwyer 2007; Dwyer et al. 2007; Gross and Acquisti 2005; Hoadley et al. 2010; Jagatic et al. 2007; Xu et al. 2008			Hodge 2006

domain. As shown in Table 2, various studies have been conducted to examine how technological applications influence privacy concerns for individuals, groups, organizations and societies.

Looking Across Contexts

Although researchers have explored privacy-related research questions in different contexts, it remains unclear that the context-specific nuances actually merit parallel research streams. In our view, the answer to Question #3 ("To what extent does context matter in the relationships between privacy and other constructs?") is "much less than a first-order consideration of the research stream would lead one to believe."

One can understand why individual researchers (especially in the IS domain) have embraced this path. Most of the new contexts are technologically driven, and thus the IT artifact and the impact of the new technological application on privacy is evident, making the research relevant for publi-

cation in IS journals. Moreover, the historical precedent of the Internet as a technology that completely changed the landscape of the privacy conversation has given scholars reason to suspect that another type of technology may once again turn around our understanding of privacy. Indeed, a similar approach is taken by legal scholars who are regularly engaged in research on how a specific new legal framework or law passed by the U.S. Congress (or another nation's legislative body) would impact privacy.

Yet we note that while these types of studies provide high relevance and illustrate the IT artifact's salience, the cumulative impact of such context-driven studies may produce an overall contribution to knowledge that is suboptimal unless researchers are constantly aware of an over-arching model. Although it is certainly necessary to ascertain the extent to which data from different contexts converge and diverge before such data are pooled, far more could eventually be learned from a macro perspective. As we will discuss in the next section, "Future Research and Conclusion," some minor parameterization of an APCO framework (as in our Figure 3) should accommodate the majority of the studies that are now context-specific. This would lead to a more robust framework that would move the frontier of knowledge forward far more quickly.

Future Research and Conclusion

We draw the following overarching conclusions from the literature review:

- A large body of normative studies of privacy has accumulated. Many of these offerings are politically engaging or emotionally charged with strong beliefs about the ethics and norms that underlie democratic societies. While these studies have contributed to privacy research in their own merit, they also serve as excellent inspiration and motivation for research advancement, bringing to light hot and disputed issues, conflicts, and contradictions. There are many rich and valid theoretical developments and models in the body of purely descriptive studies on general privacy in philosophy, sociology, and law that have not been addressed in empirical research on privacy. However, rigorous *empirically descriptive* studies that either trace processes associated with, or test implied assertions from, these value-laden arguments could add great value.

- Most of the empirically descriptive studies that have addressed linkages between antecedents and privacy concerns have focused on *individual* perceptions. For the most part, the studies that have associated privacy concerns with outcomes have been concerned with *organizational* and *societal* dynamics. Largely missing from the entire research stream are studies associated with *group*-level privacy. Future empirical studies—both positivist and interpretive—could profitably be targeted to these under-researched levels of analysis.

- Positivist empirical studies will add the greatest value if they focus on *antecedents* to privacy concerns and on *actual outcomes*. As could be seen in our discussion of Question #2, only limited attention has been paid to factors that serve as antecedents to privacy concerns. At the same time, often due to a reliance on the TRA, researchers frequently assume that stated intentions will equate to actual behaviors, an especially tenuous assumption in light of the privacy paradox.

Once the extent to which data from different contexts converge and diverge has been ascertained, attempts to forge a *context-neutral, overarching empirical framework* should be encouraged. We now discuss each of these conclusions.

Normative to Empirical

Previous research has provided a plethora of normative arguments that address conundrums ranging from the theoretical orientation of privacy (e.g., debates about the extent to which privacy is a human right and ought to be protected as such) to the regulatory approach that best serves society (e.g., debates about whether there should be a federal bureau of privacy). In between, one can find normative arguments associated with specific matters of privacy interpretation (e.g., debates about whether an IP address associated with one's home computer constitutes "individually identifiable personal data" that should be protected).

There are "rules" for what constitutes a rigorous normative argument—often grounded in principles of moral argumentation. Such arguments may include references to empirical data, but such references are not required since normative arguments can be made logically without reference to data.

The overall stream of privacy research has benefited from some of the normative argumentation that has been published. Further, some of the normative argumentation has yielded real-world significance in domains such as privacy regulation; for example, normative arguments undergirded the competing drivers for institutional structures that can be observed in the United States and the European Union. But, in our view, a general extension of the stream of normative privacy argu-

mentation is unlikely to produce many new insights in the IS domain that will augur for significant changes in policy or behavior at any of the units of analysis discussed previously: individual, group, organization, or society.

However, to the extent that the normative conclusions are viewed as enlightening and motivating events for empirical studies that *trace processes associated with the implementation of these normative conclusions or that test the impact on different outcomes*, their value rises enormously. For example, an emotionally charged assertion such as "there is war on privacy" (e.g., Sobel 1976) or "the system is broken" (Turow 2003), or a lengthy normative debate regarding whether privacy should be viewed as a right or as a commodity will yield little additional insight. The normative debates *themselves* are unlikely to inform us further in terms of privacy protection, but an examination of the positivist nomological models that link the normative conclusions to different outcomes, or the processes through which that linkage occurs, could prove quite instructive.

A natural difficulty that arises regarding tests of positivist models from normative studies is the fact that only a subset of the normative arguments lends itself to such study, since the normative conclusions are seldom stated in a format that is suitable for positivist testing. Unlike many theories in the social sciences that posit relationships such as "higher levels of A will be associated with higher levels of B," normative, value-laden arguments seldom concern themselves with whether or not they are testable. Consequently, one might observe a normative conclusion such as "societies ought to acknowledge a right to privacy in purchase transactions" without any clear linkage to outcomes that would, or would not, follow from such a right. In other words, the normative theory prescribes that higher levels of "A" should be provided. It then becomes a task for the positivist researcher to define which constructs might constitute "B" and to develop a testable linkage back to "A."

As they traverse this path, researchers should be quite explicit in identifying the assumptions on which they are relying, and they should be sure to defend those assumptions. The normative and purely descriptive studies that provide solid argumentation and reasoning can serve as bridges in constructing empirically testable models and motivating process tracing studies. As an example, many researchers rely on the set of fair information practices (FIPs) that were codified in a 1973 study by the U.S. Department of Health, Education, and Welfare, and some researchers rotate their positivist models around these FIPs. But the FIPs do not have the standing of U.S. law in any omnibus context, and careful listeners will conclude that some members of U.S. industry groups do not even embrace certain principles of the FIPs. It is, therefore, incumbent upon researchers who assume the validity of the FIPs to note this clearly in their papers and to defend why the assumption should hold for the purposes of the positivist research.

Levels of Analysis

The majority of empirical studies to date have viewed the individual as the salient unit of analysis. This is to some degree understandable, since such studies lend themselves to data collection through written and online surveys, and they are therefore easier to implement. Further, great insight can be gained from consideration of individuals' perceptions of various privacy-related activities.

However, much of this focus on individual-level privacy perceptions and relationships has been at the expense of our understanding at other levels of analysis. The challenge, of course, is that studies at the organizational and societal levels are necessarily more complex and less conducive to "quick" data collection techniques such as written and online surveys. Indeed, most rigorous studies of organizational privacy policies and practices would likely include a set of exhaustive interviews with an organization's members and stakeholders, and some amount of deep process tracing would also likely be involved. Such studies are the best approach to uncovering the somewhat subtle organizational dynamics that drive privacy policies and practices.

Cross-national and cross-cultural studies are also likely to be challenging, although one can often simplify the measurement of certain independent variables in positivist studies by considering previously established metrics. For example, many countries' privacy regulatory structures have already been documented by previous researchers. Similarly, national public opinion surveys regarding privacy concerns are available for a number of industrialized countries. While researchers may still have to struggle with some challenges when using such external data (e.g., manual adjustment of degrees of freedom for statistical inference), the structure of the studies may not be overly complex. On the other hand, interpretive studies at the cross-national and cross-cultural levels may be overwhelming in their complexity. For example, many languages, including those in European countries (e.g., Russian, French, Italian), do not have a word for *privacy* and have adopted the English word.[9] One's ability to collect interpretive (and, particularly, process-oriented) data across national and societal boundaries will ordinarily be

[9]The etymological origin of privacy is distant from its modern use: the Latin word *privus* has an archaic meaning of single and shares a common root with the word *privare*, meaning deprive.

limited, perhaps even artificially, due to historical factors. Even so, as the majority of the literature to date has focused on the United States, the relatively lesser focus and complexity of the literature in other countries may be due to the varying legal environs. Presumably, the United States has a more complex legal environment than Europe, and this may be partly the reason for the emphasis of the research on the United States. In any case, a richer focus on international dimensions of privacy research is needed.

Of particular note is that there have been very few studies that considered privacy at the small group level. Of course, it is at the small group level that many supra-organizational policies and practices come to rest, so the paucity of studies at this level strikes us as a significant weakness in the privacy literature stream. Further, within small groups (whether nestled in larger organizations or not), norms regarding protection of individuals' privacy may vary, and the process through which these norms develop could serve as an interesting area for future research. It is also likely that small groups differ in norms regarding protection of the group's own information,[10] and these differences (and the processes through which they evolve) also merit future research consideration. In a related vein, a single individual likely belongs to more than one group, so (s)he may adhere to different norms regarding privacy as (s)he travels between groups. How an individual navigates such different normative expectations would also be a fruitful domain for additional research.

In fact, social networking websites such as Facebook and Twitter offer dynamic examples in which information boundaries are created in groups of various sizes and relationship levels. One can easily imagine a set of studies that considers the factors associated with different boundaries regarding disclosure within and across online groups. Questions such as "do limited-access groups differ from open access groups in their information norms and processes?" and "to what extent does an online group's administrator's own information concerns dictate the privacy norms and processes in the group?" could be of great interest in this domain.

Additionally, as a precursor to this work, the very definition of a *group* merits consideration in light of developments in online social networking. To the extent that sociological and communications research on small groups has been undertaken in the past, it has usually been associated with physical groups in which membership is somewhat static (or, at least, easily clarified) and non-anonymous. However, online groups are often associated with fluid entry and exit, with the option of identification through screen names or anonymous avatars. In addition, what constitutes a "small" group in terms of sociology and communication (for which traditional theories were developed) may well be subject to dynamic forces. Although a physical group's characteristics may shift substantially as it grows in size, this may not be as true of an online group. Clear distinctions (and, likely, reconsiderations of nomenclature) are warranted.

Yet it is also obvious that, as with organizational studies, it will not be easy to conduct these inquiries into the privacy relationships and practices of small groups. Although some possibilities for surveys do exist, the most helpful studies will likely be grounded in direct observation of the group members and their interactions. This suggests a long-term research agenda that will rely heavily on access to group settings in a variety of domains. It will be almost impossible to examine these processes without direct observation or participation (i.e., through action research).

Antecedents and Outcomes

As suggested above, the most helpful positivist studies will be those that examine differences in outcomes as a function of privacy-related independent variables. *Outcomes* should be interpreted as actual changes of state or behavior; this is distinct from an examination of attitudes, beliefs, and intentions.

Indeed, it is rare for privacy research to consider actual outcomes in tests of models. Although some exceptions are emerging (see Cranor et al. 2007; Hui et al. 2007), the general approach has been to ascertain what subjects report that they would intend to do in a certain situation—for example, subjects might report their likelihood of writing to an elected official to complain about a perceived privacy violation (Smith et al. 1996).

Particularly because of the privacy paradox, it will behoove privacy researchers to consider their nomological models as exhaustive only when they map to actual outcomes at one or more levels of analysis. Among others, outcomes such as documented violations of privacy, successful prosecutions of privacy violations, and cross-national data flow stoppages would all serve as salient outcomes in testable models. At the organizational level, an interesting contribution would be to reveal specific organizational outcomes and consequential decisions made after breaches of personal information considered private. In contrast, much less insight would be gained through tests of models that culminate with dependent variables that are perceptual in nature—for example, a survey

[10]We refrain from referring to the concept of privacy when referring to information associated with the *group*, since privacy is best viewed as referring to information about *individuals*. Even so, norms regarding the proprietary nature of group information may vary across groups.

of subjects' differing levels of stated privacy concern as associated with different uses of personal data. To the extent that a privacy paradox exists, it is obvious that such perceptual measures are quite distinct from measures that will provide insight to decision-makers.

Overarching APCO Macro Model

Finally, we argue that positivist privacy researchers should keep their eye on an optimized APCO macro model that eventually includes an expanded set of antecedents as well as an exhaustive set of outcomes. The ultimate objective should be a macro model that will prove useful across disciplines and contexts.

It is well beyond the scope of the present endeavor to propose this full APCO macro model. As a nod to the attributes of emerging technological applications and other contextual factors, the macro model may require some amount of parameterization if contextual differences are demonstrated to be clearly salient. For example, one can envision a macro model that includes a set of antecedents that would apply to all types of personal information, such as financial and medical. Through parameterization, some of the antecedents could be hypothesized to hold with greater weight for some of the information types than for others based on findings from studies that target these contextual differences. Yet, all researchers should be aware of the exhaustive set of antecedents, as there is little need for each discipline or sector to investigate its own set of antecedents. Similarly, context parameterization could be used to highlight outcomes that would be more or less salient for different contexts.

The development of this macro model would be arduous and contentious, but the ultimate payoff for the *gestalt* of privacy research would be immense. With the macro model in place, individual researchers could then contribute studies that addressed a clear subset of the antecedents and outcomes, with possible parameterization, always confident that their findings would contribute a clearly annotated brick in the wall of privacy knowledge.

Conclusion

The stream of modern privacy research had its genesis in the 1970s. In the subsequent four decades, a number of useful studies have been conducted and published, but the overall research stream has been suboptimized because of its disjointed nature.

We believe that our recommendations for future research in privacy should lead to a more cohesive stream of literature that yields actionable steps for individuals, managers, and regulators.

Acknowledgments

The authors are very grateful to Lynne Markus, Senior Editor, for her encouragement and direction in helping them develop this manuscript. They are also grateful to the associate editor, Paul Pavlou, for his helpful guidance, and to the three anonymous reviewers for their constructive advice and very helpful comments on earlier versions of this manuscript. Heng Xu gratefully acknowledges the financial support of the National Science Foundation under grant CNS-0953749.

References

Ackerman, M. 2004. "Privacy in Pervasive Environments: Next Generation Labeling Protocols," *Personal and Ubiquitous Computing* (8:6), pp. 430-439.

Acquisti, A. 2004. "Privacy in Electronic Commerce and the Economics of Immediate Gratification," in *Proceedings of the 5th ACM Electronic Commerce Conference*, New York: ACM Press, pp. 21-29.

Acquisti, A., and Gross, R. 2006. "Imagined Communities: Awareness, Information Sharing, and Privacy on the Facebook," in *Proceedings of 6th Privacy Enhancing Technologies Symposium*, Cambridge, UK, June 28-30, pp. 36-58.

Acquisti, A., and Grossklags, J. 2005a. "Privacy and Rationality in Individual Decision Making," *IEEE Security & Privacy* (3:1), pp. 26-33.

Acquisti, A., and Grossklags, J. 2005b. "Uncertainty, Ambiguity and Privacy," in *Proceedings of the 4th Annual Workshop Economics and Information Security*, Cambridge, MA, June 2-3, pp. 2-3.

Acquisti, A., and Varian, H. R. 2005. "Conditioning Prices on Purchase History," *Marketing Science* (24:3), pp. 367-381.

Alderman, E., and Kennedy, C. 1997. *The Right to Privacy*, New York: Vintage Books.

Allen, M. W., Coopman, S. J., Hart, J. L., and Walker, K. L. 2007. "Workplace Surveillance and Managing Privacy Boundaries," *Management Communication Quarterly* (21:2), pp. 172-200.

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

Altman, I. 1977. "Privacy Regulation: Culturally Universal or Culturally Specific?," *Journal of Social Issues* (33:3), pp. 66-84.

Andrade, E. B., Kaltcheva, V., and Weitz, B. 2002. "Self-Disclosure on the Web: The Impact of Privacy Policy, Reward, and Brand Reputation," in *Advances in Consumer Research*, S. M. Broniarczyk and K. Nakamoto (eds.), Valdosta, GA: Association for Consumer Research, pp. 350-353.

Ariss, S. S. 2002. "Computer Monitoring: Benefits and Pitfalls Facing Management," *Information & Management* (39:7), pp. 553-558.

Ashworth, L., and Free, C. 2006. "Marketing Dataveillance and Digital Privacy: Using Theories of Justice to Understand Consumers Online Privacy Concerns," *Journal of Business Ethics* (67:2), pp. 107-123.

Awad, N. F., and Krishnan, M. S. 2006. "The Personalization Privacy Paradox: An Empirical Evaluation of Information Transparency and the Willingness to be Profiled Online for Personalization," *MIS Quarterly* (30:1), pp. 13-28.

Bansal, G., Zahedi, F., and Gefen, D. 2008. "The Moderating Influence of Privacy Concern on the Efficacy of Privacy Assurance Mechanisms for Building Trust: A Multiple-Context Investigation," in *Proceedings of 29th International Conference on Information Systems*. Paris, France, December 14-17.

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

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

Bellman, S., Johnson, E. J., Kobrin, S. J., and Lohse, G. L. 2004. "International Differences in Information Privacy Concerns: A Global Survey of Consumers," *Information Society* (20:5), pp. 313-324.

Bennett, C. J. 1992. *Regulating Privacy: Data Protection and Public Policy in Europe and the United States*, Ithaca, NY: Cornell University Press.

Bennett, C. J. 1995. *The Political Economy of Privacy: A Review of the Literature*, Hackensack, NJ: Center for Social and Legal Research.

Bennett, C. J., and Raab, C. D. 1997. "The Adequacy of Privacy: The European Union Data Protection Directive and the North American Response," *Information Society* (13:3), pp. 245-263.

Benson, D. 1983. "A Field Study of End User Computing: Findings and Issues," *MIS Quarterly* (7:4), pp. 35-45.

Blattberg, R. C., and Deighton, J. 1991. "Interactive Marketing: Exploiting the Age of Addressability," *Sloan Management Review* (33:1), pp. 5-14.

Bok, S. 1989. *Secrets: On the Ethics of Concealment and Revelation*, New York: Vintage.

Bowie, N. E., and Jamal, K. 2006. "Privacy Rights on the Internet: Self-Regulation or Government Regulation?," *Business Ethics Quarterly* (16:3), pp. 323-342.

Boyd, D. 2008. "Facebook's Privacy Trainwreck: Exposure, Invasion and Social Convergence," *Convergence: The International Journal of Research into New Media Technologies* (14:1), pp. 13-20.

Boyd, D., and Ellison, N. B. 2007. "Social Network Sites: Definition, History, and Scholarship," *Journal of Computer-Mediated Communication* (13:1), Article 11.

Breckenridge, A. C. 1970. *The Right to Privacy*, Lincoln, NE: University of Nebraska Press, Lincoln.

Brenton, M. 1964. *The Privacy Invaders*, New York: Coward McCann.

Bruner II, G. C., and Kumar, A. 2007. "Attitude toward Location-Based Advertising," *Journal of Interactive Advertising* (7:2) (http://www.jiad.org/article89).

Budnitz, M. E. 1998. "Privacy Protection for Consumer Transactions in Electronic Commerce: Why Self-Regulation Is Inadequate " *South Carolina Law Review* (49).

Bynum, T. 2008. "Computer and Information Ethics," in *The Stanford Encyclopedia of Philosophy* (Winter 2008 Edition), E. N. Zalta (ed.),Stanford, CA: Center for the Study of Language and Information (http://plato.stanford.edu/).

Camp, L. J. 1999. "Web Security and Privacy: An American Perspective," *Information Society* (15:4), pp. 249-256.

Campbell, A. J. 1997. "Relationship Marketing in Consumer Markets," *Journal of Direct Marketing*(11:3), pp. 44-57.

Campbell, J. E., and Carlson, M. 2002. "Panopticon.com: Online Surveillance and the Commodification of Privacy," *Journal of Broadcasting & Electronic Media* (46:4), pp. 586-606.

Caudill, E. M., and Murphy, P. E. 2000. "Consumer Online Privacy: Legal and Ethical Issues," *Journal of Public Policy & Marketing* (19:1), pp. 7-19.

Cespedes, F. V., and Smith, H. J. 1993. "Database Marketing: New Rules for Policy and Practice," *Sloan Management Review* (34:4), pp. 7-22.

Chellappa, R. K. 2008. "Consumers' Trust in Electronic Commerce Transactions: The Role of Perceived Privacy and Perceived Security," unpublished paper, Emory University, Atlanta, GA.

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

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

Clark, T. D., Jones, M. C., and Armstrong, C. P. 2007. "The Dynamic Structure of Management Support Systems: Theory Development, Research Focus, and Direction," *MIS Quarterly* (31:3), pp. 579-615.

Clarke, R. 2001. "Person Location and Person Tracking: Technologies, Risks and Policy Implications," *Information Technology & People* (14:2), pp. 206-231.

Cohen, J. E. 2001. "Privacy, Ideology, and Technology: A Response to Jeffrey Rosen," *Georgetown Law Journal* (89), p. 2029.

Consumers-Union. 2008. "Consumer Reports Poll: Americans Extremely Concerned About Internet Privacy," September 25 (http://www.consumersunion.org/pub/core_telecom_and_utilities/006189.html).

Copp, D. (ed.). 2007. *The Oxford Handbook of Ethical Theory*, New York: Oxford University Press,

Cranor, L. F. 2003. "'I Didn't Buy it for Myself': Privacy and Ecommerce Personalization," in *Proceedings of the 2003 ACM Workshop on Privacy in the Electronic Society*, Washington, DC, October 27-30, pp. 111-117

Cranor, L. F., Egelman, S., Tsai, J., and Acquisti, A. 2007. "The Effect of Online Privacy Information on Purchasing Behavior: An Experimental Study," in *Proceedings of 28th International Conference on Information Systems*, Montréal, Canada, December 9-12.

Culnan, M. J. 1985. "Consumer Awareness of Name Removal Procedures: Implication for Direct Marketing," *Journal of Interactive Marketing* (9), pp. 10-19.

Culnan, M. J. 1993. "'How Did They Get My Name'? An Exploratory Investigation of Consumer Attitudes toward Secondary Information Use," *MIS Quarterly* (17:3), pp. 341-364.

Culnan, M. J. 2000. "Protecting Privacy Online: Is Self-Regulation Working?," *Journal of Public Policy and Marketing* (19:1), pp. 20-26.

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

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

Culnan, M. J., and Williams, C. C. 2009. "How Ethics Can Enhance Organizational Privacy: Lessons from the ChoicePoint and TJX Data Breaches," *MIS Quarterly* (33:4), pp. 673-687.

D'Urso, S. 2006. "Who's Watching Us at Work? Toward a Structural–Perceptual Model of Electronic Monitoring and Surveillance in Organizations," *Communication Theory* (16:3), pp. 281-303.

Davies, S. G. 1997. "Re-Engineering the Right to Privacy: How Privacy Has Been Transformed from a Right to a Commodity," in *Technology and Privacy: The New Landscape,* P. E. Agre and M. Rotenberg (eds.), Cambridge, MA: MIT Press, pp. 143-165.

Dhillon, G. S., and Moores, T. 2001. "Internet Privacy: Interpreting Key Issues," *Information Resources Management Journal* (14:4), pp. 33-37.

Dholakia, N., and Zwick, D. 2001. "Contrasting European and American Approaches to Privacy in Electronic Markets: A Philosophical Perspective," *Electronic Markets* (11:2), pp. 116-120.

Dinev, T., Bellotto, M., Hart, P., Russo, V., Serra, I., and Colautti, C. 2006a. "Internet Users' Privacy Concerns and Beliefs About Government Surveillance: An Exploratory Study of Differences between Italy and the United States," *Journal of Global Information Management* (14:4), pp. 57-93.

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

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

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

Dinev, T., and Hart, P. 2007. "Privacy Concerns and Levels of Information Exchange: An Empirical Investigation of Intended E-Services Use," *E-Service Journal* (4:3), pp. 25-61.

Dinev, T., Xu, H., and Smith, H. J. 2009. "Information Privacy Values, Beliefs and Attitudes: An Empirical Analysis of Web 2.0 Privacy," in *Proceedings of 42nd Hawaii International Conference on System Sciences*, Los Alamitos, CA: IEEE Computer Society Press.

Dolnicar, S., and Jordaan, Y. 2007. "A Market-Oriented Approach to Responsibly Managing Information Privacy Concerns in Direct Marketing," *Journal of Advertising* (36:2), pp. 123-149.

Dwyer, C. 2007. "Digital Relationships in the 'MySpace' Generation: Results from a Qualitative Study," in *Proceedings of 40th Hawaii International Conference on System Sciences*, Los Alamitos, CA: IEEE Computer Society Press.

Dwyer, C., Hiltz, S., and Passerini, K. 2007. "Trust and Privacy Concern Within Social Networking Sites: A Comparison of Facebook and MySpace," in *Proceedings of the 13th Americas Conference on Information Systems (AMCIS)*, Keystone, CO, August 9-12.

Eastlick, M. A., Lotz, S. L., and Warrington, P. 2006. "Understanding Online B-to-C Relationships: An Integrated Model of Privacy Concerns, Trust, and Commitment," *Journal of Business Research* (59:8), pp. 877-886.

Edelman, B. 2011. "Adverse Selection in Online 'Trust' Certifications and Search Results," *Electronic Commerce Research and Applications* (1), pp. 17-25.

Etzioni, A. 1999. *The Limits of Privacy*, New York: Basic Books.

Fairweather, N. B. 1999. "Surveillance in Employment: The Case of Teleworking," *Journal of Business Ethics* (22:1), pp. 39-49.

Featherman, M. S., and Pavlou, P. A. 2003. "Predicting E-Services Adoption: A Perceived Risk Facets Perspective," *International Journal of Human-Computer Studies* (59:4), pp. 451-474.

Fishbein, M., and Ajzen, I. 1975. *Belief, Attitude, Intention, and Behavior: An Introduction to Theory and Research*, Reading, MA: Addison-Wesley.

Foxman, E. R., and Kilcoyne, P. 1993. "Information Technology, Marketing Practice, and Consumer Privacy: Ethical Issues," *Journal of Public Policy & Marketing* (12:1), pp. 106-119.

Garfinkel, S. 2000. *Database Nation: The Death of Privacy in the 21st Century*, Sebastopol, CA: O'Reilly Media.

Gomez, J., Pinnick, T., and Soltani, A. 2009. "KnowPrivacy: The Current State of Web Privacy, Data Collection, and Information Sharing," School of Information, University of California Berkeley (http://www.knowprivacy.org/).

Goodhue, D. L., and Straub, D. W. 1991. "Security Concerns of System Users: A Study of Perceptions of Ahe adequacy of Security," *Information and Management* (20:1), pp. 13-27.

Grinter, R., and Palen, L. 2002. "Instant Messaging in Teen Life," in *Proceedings of the 2002 ACM Conference on Computer Supported Cooperative Work*, New Orleans, Louisiana, pp. 21-30.

Gross, R., and Acquisti, A. 2005. "Information Revelation and Privacy in Online Social Networks," in *Proceedings of the 2005 ACM Workshop on Privacy in the Electronic Society*, Alexandria, VA,.

Häkkilä, J., and Chatfield, C. 2005. "'It's like If You Opened Someone Else's Letter': User Perceived Privacy and Social Practices with SMS Communication," in *Proceedings of the Mobile HCI Conference*, Salzburg, Austria, pp. 219-222.

Hann, I.-H., Hui, K.-L., Lee, S. Y. T., and Png, I. P. L. 2008. "Overcoming Online Information Privacy Concerns: An Information-Processing Theory Approach," *Journal of Management Information Systems* (24:2), pp. 13-42.

Henderson, H. 1999. *Privacy in the Information Age*, New York: Facts On File.

Herson, L. J. R. 1990. *Politics of Ideas: Political Theory and American Public Policy*, Long Grove, IL: Waveland Press.

Hirshleifer, J. 1980. "Privacy: Its Origin, Function, and Future," *The Journal of Legal Studies* (9:4), pp. 649-664.

Hoadley, C. M., Xu, H., Lee, J. J., and Rosson, M. B. 2010. "Privacy as Information Access and Illusory Control: The Case of the Facebook News Feed Privacy Outcry," *Electronic Commerce Research and Applications* (9:1), pp. 50-60.

Hodge, M. J. 2006. "Fourth Amendment and Privacy Issues on the New Internet: Facebook.com and Myspace.com," *Southern Illinois University Law Journal* (31), pp. 95-123.

Hoffman, D. L., Novak, T. P., and Peralta, M. A. 1999. "Information Privacy in the Marketspace: Implications for the Commercial Uses of Anonymity on the Web," *Information Society* (15:2), pp. 129-139.

Hui, K.-L., Tan, B. C. Y., and Goh, C.-Y. 2006. "Online Information Disclosure: Motivators and Measurements," *ACM Transactions on Internet Technology* (6), pp. 415-441.

Hui, K. L., Teo, H. H., and Lee, S. Y. T. 2007. "The Value of Privacy Assurance: An Exploratory Field Experiment," *MIS Quarterly* (31:1), pp. 19-33.

Ito, M., and Daisuke, O. 2003. "Mobile Phones, Japanese Youth and the Replacement of Social Contact," in *Proceedings of Front Stage/Back Stage: Mobile Communication and the Renegotiation of the Social Sphere,* R. Ling and P. Pedersen (eds.), Grimstad, Norway.

Jagatic, T. N., Johnson, N. A., Jakobsson, M., and Menczer, F. 2007. "Social Phishing," *Communications of the ACM* (50:10), pp. 94-100.

Jarvenpaa, S. L., and Leidner, D. E. 1999. "Communication and Trust in Global Virtual Teams," *Organization Science* (10:6), pp. 791-815.

Jarvenpaa, S. L., and Tiller, E. H. 1999. "Integrating Market, Technology, and Policy Opportunities in E-Business Strategy," *Journal of Strategic Information Systems* (8:3), pp. 235-249.

Jarvenpaa, S. L., Tractinsky, N., and Vitale, M. 2000. "Consumer Trust in an Internet Store," *Information Technology and Management* (1:12), pp. 45-71.

Jensen, C., Potts, C., and Jensen, C. 2005. "Privacy Practices of Internet Users: Self-Reports versus Observed Behavior," *International Journal of Human-Computer Studies* (63), pp. 203–227.

Jentzsch, N. 2001. "The Economics and Regulation of Financial Privacy: A Comparative Analysis of the United States and Europe," Working Paper, John F. Kennedy Institute.

Johnson, C. A. 1974. "Privacy as Personal Control," in *Man-Environment Interactions: Evaluations and Applications: Part 2,* D. H. Carson (ed.), Washington, DC: Environmental Design Research Association, pp. 83-100.

Junglas, A. I., and Spitzmüller, C. 2005. "A Research Model for Studying Privacy Concerns Pertaining to Location-Based Services," in *Proceedings of the 38th Hawaii International Conference on System Sciences*, Los Alamitos, CA: IEEE Computing Society Press.

Kelvin, P. 1973. "A Social Psychological Examination of Privacy," *British Journal of Social and Clinical Psychology* (12), pp. 248-261.

Kim, M.-C. 2004. "Surveillance Technology, Privacy and Social Control: With Reference to the Case of the Electronic National Identification Card in South Korea," *International Sociology* (19:2), pp. 193-213.

Kimmel, A. J. 1996. *Ethical Issues in Behavioral Research*, Boston: Blackwell Publishers.

Klopfer, P. H., and Rubenstein, D. I. 1977. "The Concept Privacy and Its Biological Basis," *Journal of Social Issues* (33:3), pp. 52-65.

Kobsa, A. 2002. "Personalized Hypermedia and International Privacy," *Communications of the ACM* (45:5), pp. 64-67.

Kobsa, A. 2007. "Privacy-Enhanced Personalization," *Communications of the ACM* (50:8), pp. 24-33.

Kobsa, A., and Schreck, J. 2003. "Privacy through Pseudonymity in User-Adaptive Systems," *ACM Transactions on Internet Technology* (3), pp. 149–183.

LaRose, R., and Rifon, N. 2006. "Your Privacy Is Assured—of Being Disturbed: Comparing Web Sites with and Without Privacy Seals," *New Media and Society* (8:6), pp. 1009-1029.

Laudon, K. C. 1996. "Markets and Privacy," *Communications of the ACM* (39:9), pp. 92-104.

Laufer, R. S., and Wolfe, M. 1977. "Privacy as a Concept and a Social Issue: Multidimensional Developmental Theory," *Journal of Social Issues* (33:3), pp. 22-42.

Lederer, S., Hong, J. I., Dey, A. K., and Landay, J. A. 2004. "Personal Privacy through Understanding and Action: Five Pitfalls for Designers," *Personal and Ubiquitous Computing* (8:6), pp. 440-454.

Lederer, S., Mankoff, J., and Dey, K. A. 2003. "Who Wants to Know What When? Privacy Preference Determinants in Ubiquitous Computing," in *Proceedings of Conferences on Human Factors in Computing Systems*, Fort Lauderdale, Florida.

Leidner, D., and Kayworth, T. 2006. "*Review*: A Review of Culture in Information Systems Research: Toward a Theory of Information Technology Culture Conflict," *MIS Quarterly* (30:2), pp. 357-399.

Ling, R. 2004. "The Coordination of Everyday Life," in *The Mobile Connection: The Cell Phone's Impact on Society*, R. Ling (ed.), Amsterdam: Elsevier, pp. 57-81.

Lu, Y., Tan, B. C. Y., and Hui, K.-L. 2004. "Inducing Customers to Disclose Personal Information to Internet Businesses with Social Adjustment Benefits," in *Proceedings of 25th International Conference on Information Systems*, R. Agarwal, L. J. Kirsch, and J. I. DeGross (eds.), Washington, DC, December 9-12, pp. 272-281.

Malhotra, N. K., Kim, S. S., and Agarwal, J. 2004. "Internet Users' Information Privacy Concerns (IUIPC): The Construct, the Scale, and a Causal Model," *Information Systems Research* (15:4), pp. 336-355.

Margulis, S. T. 1977a. "Conceptions of Privacy: Current Status and Next Steps," *Journal of Social Issues* (33:3), pp. 5-21.

Margulis, S. T. 1977b. "Privacy as a Behavioral Phenomenon: Introduction," *Journal of Social Issues* (33:3), pp. 1-4.

Margulis, S. T. 2003a. "On the Status and Contribution of Westin's and Altman's Theories of Privacy," *Journal of Social Issues* (59:2), pp. 411-429.

Margulis, S. T. 2003b. "Privacy as a Social Issue and Behavioral Concept," *Journal of Social Issues* (59:2), pp. 243-261.

Marx, G. T. 1999. "What's in a Name? Some Reflections on the Sociology of Anonymity," *Information Society* (15:2), pp. 99-112.

Marx, G. T. 2001. "Murky Conceptual Waters: The Public and the Private," *Ethics and Information Technology* (3:3), pp. 157-169.

McGinity, M. 2000. "Surfing Your Turf: For a Medium that Holds Anonymity in High Rregard, Privacy Is Fast Eroding," *Communications of the ACM* (43:4), pp. 19-21.

McLean, D. 1995. *Privacy and Its Invasion*, Westport, CT: Praeger.

McRobb, S., and Rogerson, S. 2004. "Are They Really Listening? An Investigation into Published Online Privacy Policies at the Beginning of the Third Millennium," *Information Technology & People* (17:4), p 442.

Meeks, B. N. 1997. "Privacy Lost, Anytime, Anywhere," *Communications of the ACM* (40:8), pp. 11-13.

Meeks, B. N. 1999. "The Privacy Hoax," *Communications of the ACM* (42:2), pp. 17-19.

Metzger, M. J. 2004. "Privacy, Trust, and Disclosure: Exploring Barriers to Electronic Commerce," *Journal of Computer-Mediated Communication* (9:4).

Milberg, S. J., Burke, S. J., Smith, H. J., and Kallman, E. A. 1995. "Values, Personal Information Privacy, and Regulatory Approaches," *Communications of the ACM* (38:12), pp. 65-74.

Milberg, S. J., Smith, H. J., and Burke, S. J. 2000. "Information Privacy: Corporate Management and National Regulation," *Organization Science* (11:1), pp. 35-57.

Milne, G. R. 1997. "Consumer Participation in Mailing Lists: A Field Experiment," *Journal of Public Policy and Marketing* (16:2), pp. 298-309.

Milne, G. R., and Boza, M.-E. 1999. "Trust and Concern in Consumers' Perceptions of Marketing Information Management Practices," *Journal of Interactive Marketing* (13:1), pp. 5-24.

Milne, G. R., and Culnan, M. J. 2002. "Using the Content of Online Privacy Notices to Inform Public Policy: A Longitudinal Analysis of the 1998-2001 US Web Surveys," *Information Society* (18:5), pp. 345-359.

Milne, G. R., and Gordon, E. M. 1993. "Direct Mail Privacy-Efficiency Trade-Offs Within an Implied Social Contract Framework," *Journal of Public Policy and Marketing* (12:2), pp. 206-215.

Milne, G. R., and Rohm, A. 2000. "Consumer Privacy and Name Removal Across Direct Marketing Channels: Exploring Opt-in and Opt-out Alternatives," *Journal of Public Policy and Marketing* (19:2), pp. 238-249.

Milne, G. R., Rohm, A., and Boza, M.-E. 1999. "Trust Has to Be Earned," in *Frontiers of Direct Marketing,* J. Phelps (ed.), New York: Direct Marketing Educational Foundation, pp. 31-41.

Miyazaki, A., and Krishnamurthy, S. 2002. "Internet Seals of Approval: Effects on Online Privacy Policies and Consumer Perceptions," *Journal of Consumer Affairs* (36:1), pp. 28-49.

Moon, Y. 2000. "Intimate Exchanges: Using Computers to Elicit Self-Disclosure from Consumers," *Journal of Consumer Research* (26), pp. 323-339.

Mowday, R. T., and Sutton, R. I. 1993. "Organizational Behavior: Linking Individuals and Groups to Organizational Contexts," *Annual Reviews in Psychology* (44:1), pp. 195-229.

Nissenbaum, H. 1998. "Protecting Privacy in an Information Age: The Problem of Privacy in Public," *Law and Philosophy* (17:5), pp. 559-596.

Nissenbaum, H. 1999. "The Meaning of Anonymity in an Information Age," *The Information Society* (15:2), pp. 141-144.

Norberg, P. A., and Horne, D. R. 2007. "Privacy Attitudes and Privacy-Related Behavior," *Psychology and Marketing* (24:10), pp. 829-847.

Norberg, P. A., Horne, D. R., and Horne, D. A. 2007. "The Privacy Paradox: Personal Information Disclosure Intentions Versus Behaviors," *Journal of Consumer Affairs* (41:1), pp. 100-126.

Nowak, G. J., and Phelps, J. 1992. "Understanding Privacy Concerns: An Assessment of Consumers's Information-Related Knowledge and Beliefs," *Journal of Direct Marketing* (6:4), pp. 28-39.

Nowak, G. J., and Phelps, J. 1995. "Direct Marketing and the Use of Individual-Level Consumer Information: Determining How and When 'Privacy' Matters," *Journal of Direct Marketing* (9:3), pp. 46-60.

Nowak, G. J., and Phelps, J. 1997. "Direct Marketing and the Use of Individual-Level Consumer Information: Determining How and When "Privacy" Matters," *Journal of Direct Marketing* (11:4), pp. 94-108.

O'Donoghue, T., and Rabin, M. 2001. "Choice and Procrastination," *Quarterly Journal of Economics* (116), pp. 121-160.

Odlyzko, A. 2004. "Privacy, Economics, and Price Discrimination on the Internet," in *Economics of Information Security,* L. J. Camp and S. Lewis (eds.), New York: Springer, pp. 187-211.

Pavlou, P. A. 2003. "Consumer Acceptance of Electronic Commerce: Integrating Trust and Risk with the Technology Acceptance Model," *International Journal of Electronic Commerce* (7:3), pp. 69-103.

Pavlou, P. A., and Gefen, D. 2004. "Building Effective Online Marketplaces with Institution-Based Trust," *Information Systems Research* (15:1), pp. 37-59.

Pearlson, K. E., and Saunders, C. S. 2009. *Managing and Using Information Systems* (4th ed.), Hoboken, NJ: John Wiley & Sons.

Pedersen, D. M. 1997. "Psychological Functions of Privacy," *Journal of Environmental Psychology* (17:2), pp. 147-156.

Pedersen, D. M. 1999. "Model for Types of Privacy by Privacy Functions," *Journal of Environmental Psychology* (19:4), pp. 397-405.

Peter, J. P., and Tarpey, S. L. X. 1997. "A Comparative Analysis of Three Consumer Decision Strategies," *Journal of Consumer Research* (2:1), p. 29.

Phelps, J., Nowak, G., and Ferrell, E. 2000. "Privacy Concerns and Consumer Willingness to Provide Personal Information," *Journal of Public Policy and Marketing* (19:1), pp. 27-41.

Ponemon Institute. 2007. "Database Security 2007: Threats and Priorities Within IT Database Infrastructure," Traverse City, MI (available at http://www.appsecinc.com/techdocs/whitepapers/2007-Ponemon-Database-Security-Study-Sponsored-by-Application-Security-Inc.pdf).

Posner, R. A. 1981. "The Economics of Privacy," *American Economic Review* (71:2), pp. 405-409.

Posner, R. A. 1984. "An Economic Theory of Privacy," in *Philosophical Dimensions of Privacy: An Anthology,* F. Schoeman (ed.), New York: Cambridge University Press, pp. 333-345.

Preston, J. 2004. "Judge Strikes Down Section of Patriot Act Allowing Secret Subpoenas of Internet Data," *The New York Times*, Technology Section, September 30.

Propp, K. M., and Kreps, G. L. 1994. "A Rose by Any Other Name: The Vitality of Group Communication Research," *Communication Studies* (45:1), pp. 7-19.

Qian, H., and Scott, C. R. 2007. "Anonymity and Self-Disclosure on Weblogs," *Journal of Computer-Mediated Communication* (12:4), pp. 1428-1451.

Rabin, M., and O'Donoghue, T. 2000. "The Economics of Immediate Gratification," *Journal of Behavioral Decision Making* (13), pp. 233-250.

Regan, P. M. 1995. *Legislating Privacy: Technology, Social Values, and Public Policy*, Chapel Hill, NC: University of North Carolina Press.

Rensel, A. D., Abbas, J. M., and Rao, H. R. 2006. "Private Transactions in Public Places: An Exploration of the Impact of the Computer Environment on Public Transactional Web Site Use," *Journal of the Association for Information Systems* (7:1), pp. 19-50.

Richards, N. M., and Solove, D. J. 2007. "Privacy's Other Path: Recovering the Law of Confidentiality," *Georgetown Law Journal* (96:1), pp. 123-182.

Rifon, N. J., LaRose, R., and Choi, S. M. 2005. "Your Privacy Is Sealed: Effects of Web Privacy Seals on Trust and Personal Disclosures," *Journal of Consumer Affairs* (39:2), pp. 339-362.

Rindfleisch, T. C. 1997. "Privacy, Information Technology, and Health Care," *Communications of the ACM* (40:8), pp. 92-100.

Rosen, J. 2000. *The Unwanted Gaze: The Destruction of Privacy in America*, New York: Random House.

Schoeman, F. D. 1984: *Philosophical Dimensions of Privacy: An Anthology*, New York: Cambridge University Press.

Schoenbachler, D. D., and Gordon, G. L. 2002. "Trust and Customer Willingness to Provide Information in Database-Driven Relationship Marketing," *Journal of Interactive Marketing* (16:3), pp. 2-16.

Schwaig, K. S., Kane, G. C., and Storey, V. C. 2006. "Compliance to the Fair Information Practices: How Are the Fortune 500 Handling Online Privacy Disclosures?," *Information & Management* (43:7), pp. 805-820.

Shah, J. R., White, G. L., and Cook, J. R. 2007. "Privacy Protection Overseas as Perceived by USA-Based IT Professionals," *Journal of Global Information Management* (15:1), pp. 68-81.

Shapiro, S. 1998. "Places and Spaces: The Historical Interaction of Technology, Home, and Privacy," *Information Society* (14:4), pp. 275-284.

Sheehan, K. B. 1999. "An Investigation of Gender Differences in On-Line Privacy Concerns and Resultant Behaviors," *Journal of Interactive Marketing* (13:4), pp. 24-38.

Sheehan, K. B. 2002. "Toward a Typology of Internet Users and Online Privacy Concerns," *Information Society* (18:1), pp. 21-32.

Sheehan, K. B., and Hoy, M. G. 1999. "Using E-Mail To Survey Internet Users in the United States: Methodology and Assessment," *Journal of Computer-Mediated Communication* (4:3).

Sheehan, K. B., and Hoy, M. G. 2000. "Dimensions of Privacy Concern among Online Consumers," *Journal of Public Policy & Marketing* (19:1), pp. 62-73.

Sheng, H., Nah, F., and Siau, K. 2008. "An Experimental Study on U-Commerce Adoption: The Impact of Personalization and Privacy Concerns," *Journal of Associations for Information Systems* (9:16), Article 15.

Singer, P. 1991. *A Companion to Ethics*, Hoboken, NJ: Wiley-Blackwell.

Sipior, J. C., and Ward, B. T. 1995. "The Ethical and Legal Quandary of Email Privacy," *Communications of the ACM* (38:12), pp. 48-54.

Sipior, J. C., Ward, B. T., and Rainone, S. M. 1998. "Ethical Management of Employee E-Mail Privacy," *Information Systems Management* (15:1), pp. 41-47.

Smith, H. J. 2001. "Information Privacy and Marketing: What the US Should (and Shouldn't) Learn from Europe," *California Management Review* (43:2), pp. 8-33.

Smith, H. J. 2004. "Information Privacy and its Management," *MIS Quarterly Executive* (3:4), pp. 201-213.

Smith, H. J., Milberg, J. S., and Burke, J. S. 1996. "Information Privacy: Measuring Individuals' Concerns About Organizational Practices," *MIS Quarterly* (20:2), pp. 167-196.

Sobel, L. A. 1976. *War on Privacy*, New York: Facts on File.

Solove, D. J. 2004. *The Digital Person: Technology and Privacy in the Information Age*, New York: New York University Press.

Solove, D. J. 2006. "A Taxonomy of Privacy," *University of Pennsylvania Law Review* (154:3), pp. 477-560.

Solove, D. J. 2008. *Understanding Privacy*, Cambridge, MA: Harvard University Press.

Stewart, K. A., and Segars, A. H. 2002. "An Empirical Examination of the Concern for Information Privacy Instrument," *Information Systems Research* (13:1), pp. 36-49.

Stone, E. F., and Stone, D. L. 1990. "Privacy in Organizations: Theoretical Issues, Research Findings, and Protection Mechanisms," *Research in Personnel and Human Resources Management* (8:3), pp. 349-411.

Stone-Romero, E. F., Stone, D. L., and Hyatt, D. 2003. "Personnel Selection Procedures and Invasion of Privacy," *Journal of Social Issues* (59:2), pp. 343-368.

Tabak, F., and Smith, W. P. 2005. "Privacy and Electronic Monitoring in the Workplace: A Model of Managerial Cognition and

Relational Trust Development " *Employee Responsibilities and Rights Journal* (17:3), pp. 173-189.

Tang, Z., Hu, Y. J., and Smith, M. D. 2008. "Gaining Trust Through Online Privacy Protection: Self-Regulation, Mandatory Standards, or Caveat Emptor," *Journal of Management Information Systems* (24:4), pp. 153-173.

Taylor, C. R. 2004a. "Consumer Privacy and the Market for Customer Information," *RAND Journal of Economics* (35:4), pp. 631-650.

Taylor, C. R. 2004b. "Privacy and Information Acquisition in Competitive Markets," Working Paper Series, Berkeley Olin Program in Law & Economics, Berkeley, CA (http://ideas.repec.org/p/cdl/oplwec/13271.html).

Tefft, S. K. 1980. *Secrecy: A Cross-Cultural Perspective*, New York: Human Sciences Press.

Turow, J. 2003. "Americans & Online Privacy: The System Is Broken," report from the Annenberg Public Policy Center, University of Pennsylvania.

Unni, R., and Harmon, R. 2007. "Perceived Effectiveness of Push vs. Pull Mobile Location-Based Advertising," *Journal of Interactive Advertising* (7:2) (http://www.jiad.org/article91).

Van Slyke, C., Shim, J. T., Johnson, R., and Jiang, J. J. 2006. "Concern for Information Privacy, Risk Perception and Online Consumer Purchasing," *Journal of the Association for Information Systems* (7:6), pp. 415-444.

Walczuch, R. M., and Steeghs, L. 2001. "Implications of the New EU Directive on Data Protection for Multinational Corporations," *Information Technology & People* (14:2), pp. 142-162.

Wald, M. 2004. "Airline Gave Government Information on Passengers," *New York Times*, Technology Section, January 18.

Waldo, J., Lin, H., and Millett, L. I. 2007. *Engaging Privacy and Information Technology in a Digital Age*, Washington, DC: National Academies Press.

Walsham, G. 1996. "Ethical Theory, Codes of Ethics and IS Practice," *Information Systems Journal* (6:1), pp. 69-81.

Wang, S., Beatty, S. E., and Foxx, W. 2004. "Signaling the Trustworthiness of Small Online Retailers," *Journal of Interactive Marketing* (18:1), pp. 53-69.

Warren, C., and Laslett, B. 1977. "Privacy and Secrecy: Conceptual Comparison," *Journal of Social Issues* (33:3), pp. 43-51.

Warren, S. D., and Brandeis, D. L. 1890. "The Right to Privacy," *Harvard Law Review* (4:5), pp. 193-220.

Weinstein, W. L. 1971. "The Private and the Free: A Conceptual Inquiry," in *Privacy: Nomos XIII*, J. R. Pennock and J. W. Chapman (eds.), New York: Atherton Press, pp. 624-692.

Weisband, S. P., and Reinig, B. A. 1995. "Managing User Perceptions of Email Privacy," *Communications of the ACM* (38:12), pp. 40-47.

Werhane, P. H. 1994. "The Normative/Descriptive Distinction in Methodologies of Business Ethics," *Business Ethics Quarterly* (4:2), pp. 175-180.

Westin, A. F. 1967. *Privacy and Freedom*, New York: Atheneum.

Westin, A. F. 2001. "Opinion Surveys: What Consumers Have to Say About Information Privacy," Prepared Witness Testimony, The House Committee on Energy and Commerce, W. J. "Billy" Tauzin, Chairman, May 8.

Westin, A. F. 2003. "Social and Political Dimensions of Privacy," *Journal of Social Issues* (59:2), pp. 431-453.

White, C., and Christy, D. 1987. "The Information Center Concept: A Normative Model and a Study of Six Installations," *MIS Quarterly* (11:4), pp. 450-458.

White, T. B. 2004. "Consumer Disclosure and Disclosure Avoidance: A Motivational Framework," *Journal of Consumer Psychology* (14:1/2), pp. 41-51.

Xu, H. 2007. "The Effects of Self-Construal and Perceived Control on Privacy Concerns," in *Proceedings of the 28th International Conference on Information Systems*, Montréal, Canada, December 9-12.

Xu, H., Dinev, T., Smith, H. J., and Hart, P. 2008. "Examining the Formation of Individual's Information Privacy Concerns: Toward an Integrative View," in *Proceedings of 29th International Conference on Information Systems*, Paris, France, December 14-17.

Xu, H., and Gupta, S. 2009. "The Effects of Privacy Concerns and Personal Innovativeness on Potential and Experienced Customers' Adoption of Location-Based Services " *Electronic Markets—The International Journal on Networked Business* (19:2), pp. 137-140.

Xu, H., and Teo, H. H. 2004. "Alleviating Consumer's Privacy Concern in Location-Based Services: A Psychological Control Perspective," in *Proceedings of the 25th International Conference on Information Systems*, R. Agarwal, L. J. Kirsch, and J. I. DeGross (eds.), Washington, DC, December 9-12, pp. 793-806.

Xu, H., Teo, H. H., and Tan, B. C. Y. 2005. "Predicting the Adoption of Location-Based Services: The Roles of Trust and Privacy Risk," in *Proceedings of 26th International Conference on Information Systems*, D. Avison, D. Galletta, and J. I. DeGross (eds.), Las Vegas, NV, December 11-14, pp. 897-910.

Xu, H., Teo, H. H., Tan, B. C. Y., and Agarwal, R. 2010. "The Role of Push-Pull Technology in Privacy Calculus: The Case of Location-Based Services," *Journal of Management Information Systems* (26:3), pp. 137-176.

Younger Committee Report. 1972. "Report of the Committee on Privacy," Cmnd.5012 HMSO.

Zweig, D., and Webster, J. 2002. "Where Is the Line between Benign and Invasive? An Examination of Psychological Barriers to the Acceptance of Awareness Monitoring Systems," *Journal of Organizational Behavior* (23), pp. 605-633.

Zweig, D., and Webster, J. 2003. "Personality as a Moderator of Monitoring Acceptance," *Computers in Human Behavior* (19), pp. 479-493.

Zwick, D., and Dholakia, N. 2004. "Whose Identity Is It Anyway? Consumer Representation in the Age of Database Marketing," *Journal of Macromarketing* (24:1), pp. 31-43.

About the Authors

H. Jeff Smith is the George and Mildred Panuska Professor in Business in the Department of Decision Sciences and Management Information Systems at the Farmer School of Business, Miami University, Oxford, Ohio. His research has appeared in *California*

Management Review, Communications of the ACM, Harvard Business Review, MIS Quarterly, MIT Sloan Management Review, Organization Science, and other journals. He served as an associate editor at *MIS Quarterly*. He holds a D.B.A. degree from Harvard University; his research has examined privacy and ethical issues associated with information technology and also organizational impediments to successful implementation of information technology applications.

Tamara Dinev is an associate professor and chair of the Department of Information Technology and Operations Management (ITOM), College of Business, Florida Atlantic University, Boca Raton, Florida. She received her Ph.D. in Theoretical Physics in 1997. Following several senior positions in information technology companies, her interests migrated to management information systems research and she joined the Florida Atlantic University ITOM faculty in 2000. Her research interests include information privacy, trust in online vendors, multicultural aspects of information technology usage, and information security. She published in several journals, including *Information Systems Research*, *Journal of the AIS*, *Journal of Strategic Information Systems*, *Communications of the ACM*, *International Journal of Electronic Commerce*, *European Journal of Information Systems*, *Journal of Global Information Management*, *e-Service Journal,* and *Behaviour and Information Technology*. She has received numerous best paper awards and nominations at major information system conferences.

Heng Xu is an assistant professor at the Pennsylvania State University where she is a recipient of the endowed PNC Technologies Career Development Professorship. She received her Ph.D. in Information Systems in 2005. She currently directs the Privacy Assurance Lab (PAL), and serves as associate director of the Center for Cyber-Security, Information Privacy and Trust (LIONS Center) at Penn State. Her research projects deal with the conceptualization, intervention, and design aspects of privacy and security. She is a recipient of the Faculty Early Career Development (CAREER) Award by the National Science Foundation (2010–2015). Her work has been published in several journals, including *Journal of Management Information Systems, Information & Management, Decision Support Systems, DATA BASE for Advances in Information Systems, Electronic Markets,* and *Journal of Information Privacy and Security*.