Journal of Social Issues, Vol. 59, No. 2, 2003, pp. 243–261

Privacy as a Social Issue and Behavioral Concept

Stephen T. Margulis[*]
Grand Valley State University

This introduction, to an issue on privacy as a social issue and behavioral concept, discusses what privacy is, by examining definitions and theories of privacy, and what privacy does, by reviewing the benefits of obtaining privacy and the costs of failing to achieve and of losing privacy. It provides a possible bridge between social psychological and social issues approaches to privacy and examines privacy as a social issue for Americans as citizens, health-care recipients, consumers, and employees. It then briefly explores behavioral aspects of privacy, including indicators of privacy's importance and the generally overlooked status of privacy in psychology.

This issue is primarily about privacy as a social issue and secondarily about privacy as a behavioral concept. This reflects what I have found in my readings over the last decade or so. I believe there has been an increasing level of scholarly interest in privacy as a social issue. The debate often emphasizes threats to privacy, how serious the threats are, and if and how these threats should be addressed. By comparison, there continues to be relative indifference to privacy, as a theoretical or research interest, among psychologists in general. Both themes are discussed below.

This introduction discusses what privacy is by examining issues in defining privacy and how privacy has been construed in two influential theories of privacy. It then examines what privacy does by reviewing theory and research on the benefits of obtaining privacy and the costs of failing to achieve and of losing privacy. Given this base, we suggest a bridge between psychological and social issues

[*] Correspondence concerning this article should be addressed to Stephen T. Margulis, Management Department, Seidman School of Business, Grand Valley State University, 401 W. Fulton, Grand Rapids, MI 49504-6431 [e-mail: Margulis@gvsu.edu].

I wish to thank John Adamopolous, Irene Frieze, Christine Smith, and our external reviewers for comments on drafts of this article. Special thanks to Gene Stone-Romero and Dianna Stone for supporting my initial proposal for this journal issue, and to Irene Frieze, my contributors, and especially Sharon Margulis, for their continued patience and support.

approaches to privacy and then discuss privacy as a social issue for Americans as citizens, health-care recipients, consumers, and employees. The introduction continues with a return to psychological aspects of privacy, including indicators of the importance of privacy and why privacy is important. It briefly reviews the status of privacy research and, to illustrate how current social-psychological theory and research can inform privacy, discusses research on values and attitudes and their implications for current and future privacy theory and research.

What Privacy Is: Issues in Defining Privacy

Because this issue is about privacy, it is important to consider what the term means. Privacy is an elastic concept (Allen, 1988). The psychological concept subsumes a wide variety of definitions (Margulis, 1977). Moreover, the relationships between privacy and cognate concepts (e.g., deception, secrecy, anonymity) are debatable (e.g., Margulis, this issue) because of disagreements about the boundaries of privacy as a concept. For example, many discussions of privacy emphasize it as a positive in the sense that privacy "protects behavior which is either morally neutral or valued by society" (Warren & Laslett, 1977, p. 44). However, other authors view privacy neutrally because they believe privacy can also support illegitimate activities, such as misuse of a public office (Westin, 1967) and vandalism (Altman, 1975), and morally dubious behavior like lying (Derlega & Chaikin, 1977). For example, DePaulo, Wetzel, Sternglanz, & Walker Wilson (this issue) make a strong case for how claims to privacy can provide the latitude to deceive others. They argue that everyday deceptions are aided by our tendency to honor claims others make about themselves but that our tendency also enables less scrupulous individuals to use deception to exploit others. Also, they discuss how deceptions can be used to protect privacy.

The psychological concept, as well as studies of everyday meanings of privacy (e.g., Newell, 1998), emphasize privacy as control over or regulation of or, more narrowly, limitations on or exemption from scrutiny, surveillance, or unwanted access (Allen, 1988; Margulis, 1977). Allen (1988) has called the narrower view the limited-access approach to defining privacy. However, I will use that expression for both the broader and narrower views. By comparison, privacy as a constitutional/legal concept, especially the post-1965 constitutional right of privacy, emphasizes decisional privacy, that is, the freedom to decide and to act in public or private as one deems appropriate, without government interference (Allen, 1988; Etzioni, 1999). However, the constitutional right of privacy may be a moribund constitutional principle (Garrow, 2001). The Fourth Amendment also protects privacy, specifically of people suspected of having committed a crime (McWhirter, 1994). The Fourth Amendment is consistent with a limited-access view of privacy protection because it prohibits the police, during criminal investigations, from making unreasonable searches. In privacy terms, people's expectations of privacy for their person and property, as defined by the courts, must be respected. That means the police cannot search a person or his or her property unless the police can demonstrate a good reason (called probable cause) for invading a person's privacy (that is, a judge issues a search warrant; McWhirter, 1994). The court's view of people's expectations of privacy has changed over time (McWhirter, 1994). Moreover, these legally defined expectations do not necessarily correspond with psychologically defined expectations of privacy (Kagehiro, 1990). The limited-access and decisional domains, although analytically distinct, may be conceptually related (Allen, 1988). Westin (1967) discusses decisional autonomy as an aspect of privacy and Margulis (1977) argues that privacy, by reducing personal vulnerabilities, increases a person's decisional options.

In Margulis (1977), I examined the variability in definitions of privacy, primarily in psychological analyses of privacy. Based on my examination, I inductively derived a formal definition, that is, "an abstract skeleton" of the means and ends of privacy: "Privacy, as a whole or in part, represents control over transactions between person(s) and other(s), the ultimate aim of which is to enhance autonomy and/or to minimize vulnerability" (Margulis, 1977, p. 10). This formal definition failed to note that, in the privacy literature, control over transactions usually entailed limits on or regulation of access to self (Allen, 1988), sometimes to groups (e.g., Altman, 1975), and occasionally to larger collectives such as organizations (e.g., Westin, 1967). Because I inductively derived the formal definition from a wide range of examples, it follows that the variation in specific definitions reflects how the terms and the relationships among terms, in the formal definition, were interpreted within those definitions. In individual cases, it also reflected whatever additional concepts and/or relationships a definition included. For example, "control," in the formal definition, has been interpreted as social power (Kelvin, 1973) and as personal control (Johnson, 1974). Johnson's (1974) distinction between primary (direct) and secondary (indirect) personal control over the attainment of privacy-related outcomes illustrates the use of an additional concept.

What Privacy Is: Lessons From Two Theories of Privacy

A way to examine the core of privacy is to compare the commonalities and differences in theories of privacy. The present examination draws on Margulis (this issue), who describes, compares, and evaluates Altman's (1975) and Westin's (1967) theories of privacy. (That article also discusses the privacy-secrecy linkage in Westin [1967] and the privacy-environment linkage that is central to Altman's theory of privacy.) Altman's (1975) theory of privacy focuses on privacy as a process of regulating levels of social interaction; Westin's (1967) theory of privacy focuses on the states (types) and functions of privacy.

Both theories are examples of limited-access approaches to privacy, that is, both discuss how individuals and groups control or regulate access to themselves.

Both theories describe our need for privacy as a continuing dynamic of changing internal and external conditions, to which we respond by regulating privacy, in order to achieve a desired level of privacy. In turn, achieved privacy can affect internal states and external conditions. Both agree that attempts to regulate privacy may be unsuccessful: We may achieve more or less privacy than we desired. Both agree that privacy can take many forms. Both agree that privacy has universal characteristics and that the nature of the forms that privacy can take is probably culturally specific. Both agree that privacy can support illegitimate goals (see above). Both differentiate the forms (or the how's) from the functions (or the why's) of privacy. They agree that the functions of privacy include opportunities for self-evaluation and that privacy contributes to self-identity and individuality. The principal difference is that Altman's theory is relatively inclusive of privacy phenomena but Westin's is less so, often focusing on information privacy. That two independent, well-supported theories share so much in common suggests they provide a reasonable foundation for understanding the fundamentals of privacy as a psychological concept.

What Privacy Does: Some Benefits and Costs

Having addressed what privacy is, let us turn to what privacy does, that is, what it provides. The first section discusses the benefits privacy provides. The second and third sections address the costs of failing to achieve privacy and the costs of losing it, respectively.

The Benefits of Privacy

The benefits of privacy reflect privacy's functions. At the sociopolitical level, in political democracies, privacy provides opportunities for political expression and criticism, political choice, and freedom from unreasonable police interference; it provides opportunities for people and organizations to prepare and discuss matters "in private"; it allows non-political participation in family, religion, and in other forms of association (Westin, 1967).

At the psychological level, privacy supports social interaction which, in turn, provides feedback on our competence to deal with the world which, in turn, affects our self-definition (Altman, 1975). From Westin's (1967) perspective, privacy provides opportunities for self-assessment and experimentation. It is a basis for the development of individuality. It protects personal autonomy. It supports healthy functioning by providing needed opportunities to relax, to be one's self, to emotionally vent, to escape from the stresses of daily life, to manage bodily and sexual functions, and to cope with loss, shock, and sorrow. In sum, privacy is important because it is posited to provide experiences that support normal psychological functioning, stable interpersonal relationships, and personal development.

The Costs of Not Obtaining Privacy

Not obtaining privacy could result in the loss of opportunities that the functions of privacy provide. They are lost because people, for physical or cognitive reasons, fail to psychologically control privacy-related behaviors (Johnson, 1974) or because people are in settings, such as an adult in a closed institutional setting or a child in a family situation, in which powerful others control or try to control the person's privacy (Goffman, 1961; Wolfe & Laufer, 1974). Short-term consequences include learning the limits of autonomy. A long-term consequence is coming to believe that certain opportunities for privacy are simply not available (Wolfe & Laufer, 1974). In psychiatric settings, long-term consequences include de-individuation and dehumanization, which undermine rehabilitation, and the loss of the ability, after release, to successfully reintegrate into ordinary life (Goffman, 1961; Ingham, 1978). Unfortunately, it appears that relatively little has been published about developmental aspects of privacy and about if and when the consequences of not obtaining desired privacy are remediated by later opportunities for privacy.

Many theories of privacy posit that psychological control is a precondition for obtaining and maintaining privacy (e.g., Altman, 1975; Johnson, 1974; Wolfe & Laufer, 1974). It follows that privacy failures include costs arising from failures of control as such. These costs could include stress (Johnson, 1974; Stone-Romero, Stone, & Hyatt, this issue) and negative feedback about personal competence. Privacy theorists have failed to integrate the rich literature on psychological control (e.g., Weary, Gleicher, & Marsh, 1993) into their theories of privacy (with Johnson, 1974, a notable exception).

The Costs of Losing Privacy

When privacy is invaded or violated, it is lost. Invasions occur when initial conditions for privacy are not achieved. Examples include being surreptitiously overheard or being unable to prevent physical access to self. Violations of privacy occur when recipients disclose to others the private information intentionally shared with them or which they obtained through an invasion of privacy. Examples include gossip and whistle-blowing. Invasions and violations of privacy result in anticipated and actual consequences (costs) of having one's "private" information or one's self in "the wrong hands." Costs presumably vary considerably, depending on many factors, especially the content of the information (Margulis, 1979; see Johnson, 1974, for a discussion of losses of privacy with favorable outcomes).

Studies of stigma illustrate privacy-related costs. Stigma can be bodily (e.g., deformities), characterological (e.g., homosexuality), and demographic (e.g., race; see Alpert, this issue, on the discrediting potential of genetic markers). However, what is relevant here is the distinction between being discredited (i.e., a person whose stigma is either previously known or is evident to co-present others) and discreditable (i.e., a person whose stigma is not known or evident; Goffman, 1963). Because stigmas are not socially acceptable and, as a result, stigmatized individuals have been devalued, been accorded lower status, and been targets of negative stereotypes, prejudice, and discrimination (Crocker, Major, & Steele, 1998), the key social problem for the discredited is managing social interaction and for the discreditable it is managing information about the stigma (Archer, 1985).

In public, discredited individuals experience invasions of privacy because the unstigmatized treat them as if it was legitimate to approach, touch, stare at, and interrogate them at will. If they fail to manage their social interactions, they experience embarrassment and feel unwanted (Archer, 1985). Derlega, Winstead, Greene, Serovich, and Elwood (2002) studied the perceived costs of failure to manage information about HIV and AIDS status, a discreditable stigma. They found that the greater a seropositive adult's belief that the public stigmatized HIV, the more strongly he or she endorsed reasons (i.e., costs such as shame and fear of rejection) for not disclosing his or her status to a parent, intimate partner, or friend. However, concealing one's HIV status is highly stressful and stress encourages HIV progression (Leary & Schreindorfer, 1998).

Losses of privacy have the potential for life-and-death costs when a person has as a critical goal the concealment of his or her intentions (e.g., moles and double agents; Richelson, 1995) or identity. For example, during World War II, Stevens (2001), a Jewish male, passing as Christian, worked for the Nazis during the day and served in an anti-Semitic, anti-Nazi Polish underground group at night.

In sum, the benefits of privacy arise from achieving its functions and its costs arise from failures to obtain or maintain privacy. However, the benefits and costs, with few exceptions, are predicted or potential, rather than demonstrated. We now turn from what privacy is and some of what privacy does to a consideration of privacy as a social issue.

Privacy as a Social Issue

The "Social" Nature of Privacy and Its Implications

Privacy is social in two senses: the social-psychological and the social-political. This duality is a bridge between social-psychological privacy as social behavior and socio-political privacy as a social issue. Social psychologically, privacy is social in three ways (cf. Shaw & Costanzo, 1970, pp. 3–5). (a) Privacy's foci are interpersonal communication and social interaction. This view of "social" predominates (see above). There are two less frequent referents. (b) How we experience, understand, react to, and enact privacy are products of our social and cultural development (Margulis, this issue). (c) Privacy is an attribute not only of individuals but also of groups and, for some theorists, organizations (see above). Regan (1995, pp. 220–231), examining privacy in a public policy (congressional) context, hence with privacy as a social-political issue, discusses the social importance of privacy at the societal level. Privacy is societally important in three ways. (a) People have a common or shared interest in privacy and in a right to privacy. Regan (1995) and Westin (this issue) summarize polling data indicating broad public support for privacy. For example, Louis Harris Polls (2000) reports that 78% of respondents to a 1990 poll agreed that the Declaration of Independence, if rewritten today, would probably include privacy as a fundamental right. (b) Privacy is a societal value because it supports and is supported by a democratic political system (for illustrations, see "The Benefits of Privacy," above; Regan, 1995; Westin, this issue). (c) Privacy is a societal good because institutional, "technological and market forces make it increasingly difficult for any one person to have privacy unless everyone has a similar minimum level of privacy" (Regan, 1995, p. 213). Regan's social-political perspective on privacy's social importance is at the intersection of social psychology and political science (cf. Kinder, 1998, p. 797).

Regan (1995) also observes that politicians and the public agree that the important threats to privacy have arisen from organization-individual relationships, hence are in the public (societal) realm, and not from informal social relationships that are in the private (individual) realm. As I note below, such organizational threats have contributed to making privacy into a social issue (also see Culnan & Bies, this issue; Marx, this issue; Westin, this issue).

Regan proposes that, to more effectively argue the value of privacy in policy-making debates, privacy should be presented as a social (societal), not an individual, value (see Regan, 1995, pp. 231–241). Her proposal is a response to her finding that framing privacy as an individual right (value, interest) had a weak impact on congressional policy-making on technological threats to privacy. One reason was that framing privacy as an individual right enabled those with competing concerns (specifically, governmental or business groups that would bear the costs of proposed privacy legislation) to eventually shape privacy legislation by invoking social interests, that is, by asking that "individual" privacy interests be balanced with interests that served the public good, such as effective law enforcement, organizational efficiency, and business competitiveness.

Regan's (1995) analysis implies that the political efficacy of social psychological privacy research may depend, in part, on researchers' ability to present their data or proposals in terms of the societal, not individual, value of privacy. A potentially weaker alternative for researchers is to present a balance between "individual" privacy and other affected values (see Culnan & Bies, this issue; Stone-Romero, Stone, & Hyatt, this issue). The potential weakness arises when privacy advocates confront economically and/or politically more powerful competitors. Then, the balance all too often has tilted away from fully satisfying privacy needs (Regan, 1995; Alpert, this issue). Gandy (this issue) might add, albeit ironically, that public opinion data, as an indicator of a common interest in privacy, are more likely to be persuasive if the polling questions are designed to provide or to support a viable policy position.

Three Positions on Privacy as a Social Issue

Westin (this issue) describes three empirically differentiated positions on privacy the public holds. I would add that these positions are also at the core of the current scholarly debate about privacy. The High-Privacy position assigns a high(er) value to privacy claims and seeks comprehensive governmental interventions to protect privacy. (See Bennett, 1995, for an overview, and Lyon & Zureik, 1996, for examples, of one approach to the High-Privacy position.) The Balanced-Privacy position values privacy claims but advocates tailored (e.g., sectoral) governmental interventions to address demonstrated abuses as well as voluntary organizational initiatives to promote individual privacy. (See Etzioni, 1999, and Westin, 1967, for different approaches to Balanced-Privacy.) The Limited-Privacy position usually assigns a lower value to privacy claims than to business efficiency and societal-protection interests and it opposes governmental intervention as unnecessary and costly. (For an example, see Singleton, 1998.) Because all but one of this issue's authors/first authors have a long-standing interest in privacy, and many contribute to the scholarly debate about privacy, they, like others, have positions on privacy. They represent the Balanced- and High-Privacy positions and stances in-between. Some (but not all) of their articles reflect their positions and some reflections are relatively obvious and others are far less so. To illustrate these positions, I will contrast the High-Privacy and Balanced-Privacy positions on certain social issues in the next section.

Westin (this issue) also provides an overview of privacy as a social issue. His framework is the political and socio-cultural role of privacy in political democracies, particularly the United States. He uses this framework to organize a contemporary history of privacy in the United States from World War II to 2002 (the year the article was completed). Westin's historical analysis tracks four factors that Westin believes drive privacy concerns. They are new technologies and their uses by government and business, social climate and public attitudes, interest group activities and policy debates, and organizational policies and federal laws. He addresses the impact of privacy concerns on Americans as citizens, employees, consumers, and as patients in our health-care system.

Current Social Issues

This section discusses four foci of concern about privacy as a social issue. They are the government's role as a threat to and defender of privacy, consumer privacy, medical and genetic privacy, and workplace privacy (cf. Westin, this issue).

Citizen Privacy and the Federal Government

Westin (this issue) traces the rises and falls of citizen attitudes about how the federal government has been affecting citizen privacy. Two central concerns have been actual, perceived, or potential threats to privacy posed by the executive branch through its extensive collection of personal information and by actions against citizens from investigative/intelligence agencies, like the FBI. In 1995, 51% of survey respondents indicated they worried "the most" about governmental invasions of privacy activities whereas 43% were worried "the most" about business activities that invade privacy. (Yet, a 1996 poll indicated that among those who said they had been victims of "an improper invasion of privacy," 43% blamed it on a business and only 13% on the government [Louis Harris Polls, 2000].)

With regard to information privacy, in spite of legislative safeguards to protect citizen privacy when federal agencies exchanged data (Westin, this issue), these laws also legitimated the use of personal information by the government for a purpose other than that for which it was collected (Regan, 1995)—a violation of privacy. In some instances, in the name of efficiency and reducing waste and fraud, some legislation undermined information privacy (Regan, 1995; for examples of privacy legislation, see Regan, 1995, and Westin, this issue).

With regard to investigative threats to citizen privacy, the federal government's response to the 9/11 terrorist attacks on the World Trade Center and Pentagon includes legislation and Department of Justice decisions that could threaten civil liberties in order to aid in catching terrorists before they can act against us. For example, the USA PATRIOT Act of 2001 (Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001), provides the executive branch with enhanced and largely unchecked surveillance and intelligence gathering ability, including tracking e-mail and Internet use and obtaining sensitive personal records. Also, it allows covert searches of a person's home and office without notifying the target of a warrant until after the search, a possible weakening of Fourth Amendment protections against unreasonable searches (Chang, 2001). However, because citizens are fearful, they want strong federal protection. I agree with Westin (this issue) that public acceptance of such measures will depend on the level of terrorist threat and on the nature and extent of actual abuse of civil liberties.

Factors affecting federal policy development (e.g., legislation) are Gandy's (this issue) focus. He describes the web of relationships between federal legislators, interest groups, and the public who are represented by public opinion polls. He examines the uses of polls about consumer privacy issues, particularly during congressional hearings, by advocates of various positions on consumer privacy. Gandy concludes that private corporations, as an interest group and a primary sponsor of privacy polls, seem to steer polls *and* the uses of polling results to promote their own positions on consumer information privacy. Gandy's examination adds to our understanding of how interest groups shape government policy (also see Regan, 1995).

Last, the U.S. government's negotiations with the European Union (EU) about how to handle transborder transfers of our personal information have become an international political issue. Regan (this issue) addresses this topic. She describes the on-going attempts of the United States and European Commission (EC) to harmonize their positions on how to protect personal information that moves between the United States and much of Europe. She considers a range of factors that affect positions on transborder data flows.

Genetic Privacy

Genetic results have become a social issue because they affect access to health and life insurance and to employment (e.g., Murry, Wimbush, & Dalton, 2001; Regan, 1996). The concern is reflected also in public opinion polls. Although one poll found 59% of respondents were likely to take advantage of genetic testing (cited in "Genetic Testing," 1999), a 1998 national poll found 63% of respondents would not take a genetic test if employers and health insurers could get access to the test results and a 1995 study found that 10% of respondents had avoided getting genetic screening for diseases, the early detection and treatment of which could have improved their lives, because they feared workplace discrimination (cited in Goldberg, 2001). Moreover, there has been overall weakness in legislative protection of health-information privacy (e.g., Rothstein, 1997b). Consequently, genetic/medical privacy has become a major policy battleground. That conclusion is best illustrated by Congress' active involvement in finalizing the most comprehensive regulation on health information privacy, the just released (August 2002) medical privacy rule (U.S. Department of Health and Human Services, 2002). Not surprisingly, Congress had been caught between pressures to change privacy provisions that were alleged to be impractical and burdensome for current health industry practice, a position endorsed by the Bush administration, and pressures to retain privacy provisions in order to protect medical and genetic privacy, which was the position of the Clinton administration. Congress changed provisions (i.e., balanced competing interests, said the health industry; weakened privacy protections, said privacy advocates; e.g., Goldstein, 2002; also see Alpert, this issue).

Alpert (this issue) discusses the privacy and policy implications for medical care, group identity, and familial relationships that are resulting from the ongoing shift to electronic medical records that will increasingly contain highly detailed genetic information. The public policy implication she discusses focuses on the federal regulation of medical privacy. (For additional information, see Westin, this issue, on the rise of genetic and medical privacy as pressing social issues; Gellman, 1999, for an overview of medical privacy issues; and Rothstein, 1997a, for a comprehensive examination of genetic privacy.)

Consumer Privacy

Culnan and Bies (this issue) discuss the competing interests of businesses, to collect and use personal information to gain and maintain a competitive advantage, and consumers, who regard certain collection-and-use practices as unfair, as invasions of privacy, or both. The authors, drawing extensively on the social psychology of justice, conclude that fair information practices (FIPs) operationalize justice concerns and balance business and consumer interests by providing the consumer with control and voice. The authors discuss three approaches to implementing FIPs: legislation and regulation, industry self-regulation (e.g., third-party assurance), and technological solutions (e.g., P3P).

Culnan and Bies (this issue) argue that consumer privacy as a social issue for Americans has its roots in technological advancements (cf. Westin, this issue). These technologies create potential threats to personal information because businesses, online and off, capture transaction information (cf. Singleton, 1998). For example, majorities of respondents (54%–89%, across three polls) object to Web tracking of their site visits, especially when identifying information is linked with tracking data (Electronic Privacy Information Center [EPIC], 2002). The threats to privacy come for companies that do not implement FIPs (Culnan & Bies, this issue) and from uninformed visitors. For example, 56% of respondents to a poll were unfamiliar with cookies, a basic tracking method (EPIC, 2002). Additionally, sophisticated software for mining increasingly large databases of personal information allows marketers to create electronic profiles of individuals (Bennett, 1995). These profiles allow customized marketing of goods and services (or, in principle, of ideologies, policies, and candidates; e.g., Larson, 1992).

Consumer privacy provides an opportunity to compare High-Privacy and Balanced-Privacy positions. (See Singleton, 1998, for a Limited-Privacy perspective.) Three comparisons follow. The Balanced-Privacy position promotes the value of FIPs. Providing notice, choice, access, and security are regarded in the United States as appropriate and sufficient for addressing consumer privacy concerns. (The four elements are discussed in Culnan & Bies, this issue.) Americans support these principles (Culnan & Bies, this issue). For example, in a 2000 poll, 88% of respondents endorsed obtaining consent (i.e., providing notice) before sharing personal information (EPIC, 2002). However, some High-Privacy advocates reject the adequacy of current FIPs as safeguards. For example, Marx (1999) believes current FIPs are insufficient because we are in a period of increasingly intrusive and expanded data-collection and use, transborder data flows, Internet usage, and other attacks on personal information. He advocates a far more comprehensive set of FIPs.

Moreover, the Balanced-Privacy and High-Privacy position differ on the nature of the controls that FIPs should provide. The opt-out approach allows a vendor to use a consumer's information unless that consumer objects. The opt-in approach requires affirmative consent from the consumer to use the consumer's information (Culnan & Bies, this issue). Most businesses and the offline world favor opt-out (Culnan & Bies, this issue; Regan, this issue). High-Privacy advocates (e.g., Davies, 1999) and the public (at least 85% support across three polls since 2000; EPIC, 2002) favor opt-in because it puts control in the hands of the affected individuals. Westin (this issue) predicts a mix of opt-in and opt-out based on the sensitivity of the information. Interactive computer technology may make a policy choice between the two, when online, unnecessary (Gellman, 1999; cf. Culnan & Bies, this issue).

What is a fair exchange for personal information? Culnan and Bies (this issue) emphasize a non-monetary exchange of personal information, based on fair information practices, in return for better service, discounts, or the like. However, some High-Privacy proponents (e.g., Rule & Hunter, 1999) also want a monetary exchange; they want consumers to share the financial benefits that result from the commercial use of their personal information.

In sum, there are two major unresolved questions about consumer privacy: How should consumer privacy issues be addressed and what are the consequences of not addressing them? For discussions of these questions, see Culnan and Bies (this issue), Jennings and Fena (2000), and Westin (this issue).

Employee Privacy

A central workplace privacy topic is the collection, storage, and use of information about the person or the person's activities, with or without the employee's consent or knowledge (Stone & Stone, 1990; Stone & Stone-Romero, 1998). This topic subsumes employee selection, placement, and promotion (see Stone-Romero, Stone, & Hyatt, this issue), measuring and controlling employee work performance, controlling or preventing deviant (e.g., illegal) behavior, and employer polices and employee strategies for protecting personal privacy (see Stone & Stone, 1990, pp. 364–381). Westin (this issue) summarizes polls that found high (76%) respondent approval of employer information practices along with sizable (30%) concern about employers' handling of employee information. Employee concerns are justified because some employers invade employees' information privacy, often without notifying their employees. For example, in a survey of major private corporations (Linowes, 1996), nearly 40% of corporations reported they lacked policies about informing employees about the types of records maintained on them, the use of the records, and on disclosures to government inquirers. Nearly 50% said they, at times, collect information on employees without prior notification.

A relatively unresearched topic is the views of employees and managers about the invasiveness and organizational value of commonly used selection procedures. However, Stone-Romero, Stone, and Hyatt (this issue) report three studies on the privacy invasiveness of 12 commonly used selection procedures. Using employed adults as respondents, two studies report consistent judgments of perceived invasiveness. A third study provides a managerial view of the invasiveness of the 12 procedures and the extent to which they protect organizational interests. Because invasiveness and organizational value were related, the authors detail the implications for organizations of choosing to use particular selection procedures.

Electronic Performance Monitoring (EPM). EPM is a form of surveillance: It can involve computer technology that monitors the use of computer and electronic equipment or the use of closed-circuit cameras to monitor workers. Although relatively small percentages of companies engage in specific EPM procedures (e.g., 19% tape phone conversations, 15% store and review e-mails, 34% use video cameras to monitor employee activities), 63% of companies engaged in at least one of the eight EPM practices that were studied (American Management Association, 1997). One aim of EPM is to monitor behavior, in contrast to work performance, in order to detect and prevent deviant or illegal activities, such as non-work-related use of equipment or drug use. Also EPM can be used to monitor work performance for purposes of work scheduling, formative or summative evaluation, or data collection to help improve organizational performance (see Aiello, 1993, and Aiello & Kolb, 1995, for summaries of issues).

Agre (1994) describes two privacy models of information collection. The surveillance model is predicated on surveillance as an intentional, often surreptitious, and malevolent basis for social control. The capture model is predicated on collecting and using information with neutral, perhaps positive, goals, such as improving organizational or system functioning. The application of EPM for monitoring work performance illustrates both models, depending on how the EPM system is designed and used (e.g., Was the system designed and implemented with employee participation, is it used with employees' knowledge and consent?) and the employer's goals (e.g., Is the goal to control performance, schedule work, appraise and reward performance or improve performance? e.g., Aiello, 1993). When the employer's goal is the social control of workers, one finds job stress, worker antipathy, and increased media attention (Aiello & Kolb, 1995; Griffith, 1993). When the goals are neutral, or positive (e.g., EPM use is aligned with employee goals), it can result in employee acceptance (Griffith, 1993). In sum, work monitoring, even if it appears to threaten employee privacy, if used in ways that are aligned with employee goals, is likely to be accepted by employees. (For a discussion of other central workplace privacy issues, see Stone & Stone, 1990, and Stone & Stone-Romero, 1998. For a discussion of privacy in employment law, see Finkin, 1995.)

This section discussed privacy as a social issue. The next section discusses privacy as a behavioral concept. Marx's (this issue) article bridges these two faces of privacy. He describes the social issue of the organizational surveillance (monitoring) of individuals in order to collect personal information and the reasons why the advantages of total monitoring are limited. His focus, however, is social-psychological; specifically, Marx presents and illustrates 11 behavioral techniques that individuals use to subvert or neutralize surveillance. He explores, also, the as-yet unexamined implications of his analysis of how individuals neutralize surveillance. Marx's approach to social psychological analysis is, in my opinion, similar to that of his mentor, Erving Goffman (cf. Marx, 1984).

Privacy as a Behavioral Concept

We return to psychological aspects of privacy, specifically to indicators of the importance of privacy and a brief review of the status of privacy in several disciplinary areas of psychology.

The Behavioral Sciences and the Importance of Privacy

Having reviewed the social (societal) importance of privacy as a social issue, we turn to privacy's importance as a behavioral phenomenon. The strongest and most controversial support are (a) Altman's (1977) conclusion that privacy may be a cultural universal (also see Nucci, 1997) and (b) Klopfer and Rubenstein's (1977) conclusion that privacy may be a "universal" in mammals and birds. Support for Klopfer and Rubenstein is provided by studies of a wide range of species of the mechanisms used by prey to avoid detection by predators (Krebs & Davies, 1993). Support for Altman's position is provided by Moore's (1984) conclusion that privacy could be a universal in nonliterate societies and by studies of privacy in different societies in Asia (e.g., Chan, 2000; Iwata, 1988) and Africa (e.g., Idehen, 1997; Newell, 1998). In sum, forms of privacy are (probably) found throughout the world. Neverthless, most of what we know about privacy, with this issue a case in point, draws on North American and European societies in which the individualist cultural model prevails. This model emphasizes the autonomous individual, choice and control, and social relationships as either voluntary or as barriers to independence (Fiske, Kitayama, Markus, & Nisbett, 1998). The limited-access approach to privacy, with its emphasis on choice and control and, implicitly, the autonomous individual, reflects elements of this model. The individualist model and privacy have been linked by Etzioni (1999), Triandis (1995) and Westin (1967).

Three other studies are germane to privacy's importance as a behavioral phenomenon. Argyle, Henderson, and Furnham (1985), in a study of 33 social rules, found that the two of the three most widely applicable rules across 22 types of relationships (e.g., spouse, teacher) were privacy-related: respecting other's privacy, and not discussing what one is told in confidence. The third rule was looking others in the eye during conversations. Diaz-Veizades, Widaman, Little, and Gibbs (1995) reported four cross-validated factors that represent human rights attitudes: privacy, equality (equal access to basic rights), civilian constraint (the acceptability of limiting civil and political rights), and social security (access or entitlement to an adequate standard of living). Krämer (1995), using multidimensional scaling, identified three criteria that determine preferences for generic places (e.g., art gallery, hospital). The criteria were the function of places (e.g., residential, service), the specificity of the function (whether functions were obligatory or additional), and the privacy. In sum, privacy appears to be important across a range of behavioral areas, societies, and species.

The Status of Privacy

This section briefly summarizes the status of privacy in social, environmental, and in industrial/organizational (I/O) psychology. In social psychology, self-disclosure has long been linked to privacy (e.g., Derlega & Chaikin, 1977). A case can be made for linking psychological control (Johnson, 1974) and secrecy (Margulis, this issue) to privacy. Bercheid (1977) concluded that social psychologists have studied many topics, such as social facilitation, attitude formation and change, social influence, deindividuation, and social comparison processes, that address privacy-related issues "but which are often overlooked as privacy related" (p. 85). Being overlooked may be the key to privacy's status in social psychology. For example, Berscheid's conclusion is reflected, 20 years later, in the current *Handbook of Social Psychology* (Gilbert, Fiske, & Lindzey, 1998). Privacy received scant notice—four references to "privacy" and "private" in the indexes and usually passing coverage in the text. An exception is DePaulo et al.'s (this issue) integration of social psychological research on deception with the concept of privacy. Similarly, Stone and Stone (1990) have concluded that I/O psychologists continue to neglect privacy. By comparison, environmental psychologists have had a sustained interest in privacy (Altman, 1975; Margulis, this issue). I believe those interested in privacy and those interested in other psychological phenomena and processes can profit from drawing on each other's concepts and research findings and systematically incorporating that information into their own theories and research.

The Organization of the Current Issue

Articles on social issues appear first, moving from international, to national, to institutional/organizational issues. *Regan* discusses international aspects of privacy, specifically, EC-U.S. differences in protecting personal information in transborder data flows. Gandy and Alpert focus on federal policy development. *Gandy* discusses the relationships between public opinion poll sponsorship, polling results, and the use of polling data in congressional hearings. *Alpert* discusses threats to medical and genetic privacy and the HIPPA privacy rule, a regulation meant to protect health information privacy. *Culnan and Bies* examine consumer issues involving online commerce and apply social-psychological theories of justice to create greater consumer trust in online vendors. *Stone-Romero, Stone, and Hyatt* examine workplace privacy. The article presents three empirical studies that address employees' and managers' perceptions of the invasiveness and organizational value of employment selection tests. *Marx* provides a transition between the social issues and behavioral sections. His focus is the social issue of surveillance and the individual behavioral techniques people use to neutralize surveillance. *DePaulo, Wetzel, Sternglaz, and Walker Wilson* review the literature on deception from a privacy perspective and conclude that the two are linked. *Margulis* evaluates the influence of and empirical support for the privacy theories of two leading privacy theorists, Westin and Altman, and examines Westin's linkage of privacy and secrecy and Altman's contribution to the linkage between privacy and the environment. *Westin* ends the issue with a social and political history of privacy in the United States since World War II. He indicates where the aforementioned articles fall within his framework and in his account of social issues.

References

Agre, P. E. (1994). Surveillance and capture: Two models of privacy. *The Information Society, 10*(2), 101–127.

Aiello, J. R. (1993). Computer-based work monitoring: Electronic surveillance and its effects. *Journal of Applied Social Psychology, 23*, 499–507.

Aiello, J. R., & Kolb, K. J. (1995). Electronic performance monitoring: A risk factor for workplace stress. In S. L. Sauter & L. R. Murphy (Eds.), *Organizational risk factors for job stress* (pp. 163–179). Washington, DC: American Psychological Association.

Allen, A. L. (1988). *Uneasy access: Privacy for women in a free society*. Totowa, NJ: Rowman & Littlefield.

Altman, I. (1975). *The environment and social behavior: Privacy, personal space, territory, crowding*. Monterey, CA: Brooks/Cole.

Altman, I. (1977). Privacy regulation: Culturally universal or culturally specific? *Journal of Social Issues, 33*(3), 66–84.

American Management Association. (1997). Electronic monitoring & surveillance. Retrieved December 1999 from http://www.amanet.org/survey/elec97.htm

Archer, D. (1985). Social deviance. In G. Lindzey & E. Aronson (Eds.), *The handbook of social psychology* (3rd ed., Vol. 2, pp. 743–804). New York: Random House.

Argyle, M., Henderson, M., & Furnham, A. (1985). The rules of social relationships. *British Journal of Social Psychology, 24*, 125–139.

Bennett, C. J. (1995). *The political economy of privacy: A review of the literature*. Paper prepared for the Center for Social and Legal Research, DOE Genome Project (Final draft). Victoria, BC: University of Victoria, Department of Political Science.

Berscheid, E. (1977). Privacy: A hidden variable in experimental social psychology. *Journal of Social Issues, 33*(3), 85–101.

Chan, Y-K (2000). Privacy in the family: Its hierarchical and asymmetric nature. *Journal of Comparative Family Studies, 31*(1), 1–17.

Chang, N. (2001, November). *The USA PATRIOT Act: What's so patriotic about trampling on the Bill of Rights?* Retrieved April 2002 from http://www.ccrny.org.whatsnew/usa_patriot_act.asp

Crocker, J., Major, B., & Steele, C. (1998). Social stigma. In D. T. Gilbert, S. T. Fiske, & G. Lindzey (Eds.), *The handbook of social psychology* (4th ed., Vol. 2, pp. 504–553). Boston: McGraw-Hill.

Davies, S. (1999). Spanners in the works: How the privacy movement is adapting to the challenge of Big Brother. In C. J. Bennett & R. Grant (Eds.), *Visions of privacy: Policy choices for the digital age* (pp. 244–261). Toronto, Ontario, Canada: University of Toronto Press.

Derlega, V., & Chaikin, A. L. (1977). Privacy and self-disclosure in social relationships. *Journal of Social Issues, 33*(3), 102–115.

Derlega, V. J., Winstead, B. A., Greene, K., Serovich, J., & Elwood, W. N. (2002). Perceived HIV-related stigma and HIV disclosure to relationship partners after finding out about the seropositive diagnosis. *Journal of Health Psychology, 7*(4), 415–432.

Diaz-Veizdes, J., Widaman, K. F., Little, T. D., & Gibbs, K. W. (1995). The measurement and structure of human rights attitudes. *Journal of Social Psychology, 135*(3), 313–328.

Electronic Privacy Information Center [EPIC]. (2002). *Public opinion on privacy*. Retrieved May 2002 from http://www.epic.org/privacy/survey/default.html

Etzioni, A. (1999). *The limits of privacy*. New York: Basic Books.

Finkin, M. W. (1995). *Privacy in employment law*. Washington, DC: BNA Books.

Fiske, A. P., Kitayama, S., Markus, H. R., & Nisbett, R. E. (1998). The cultural matrix of social psychology. In D. T. Gilbert, S. T. Fiske, & G. Lindzey (Eds.), *The handbook of social psychology* (4th ed., Vol. 2, pp. 915–981). Boston: McGraw-Hill.

Garrow, D. J. (2001). Privacy and the American constitution. *Social Reseach, 68*(1), 55–82.

Gellman, R. (1999). Personal, legislative, and technical privacy choices: The case of health privacy reform in the United States. In C. J. Bennett & R. Grant (Eds.), *Visions of privacy: Policy choices for the digital age* (pp. 129–145). Toronto, Ontario, Canada: University of Toronto Press.

Genetic testing: "Minefield" of potential legal liability for employers. *Employee Benefit Plan Review, 53*(11), 41–42.

Gilbert, D. T., Fiske, S. T., & Lindzey, G. (Eds.). (1998) *The handbook of social psychology* (4th ed.). Boston: McGraw-Hill.

Goffman, E. (1961). *Asylums*. Garden City, NY: Anchor.

Goffman, E. (1963). *Stigma: Notes on the management of spoiled identity*. Englewood Cliffs, NJ: Prentice-Hall.

Goldberg, I. V. (2001). Genetic information privacy and discrimination. *The Health Care Manager, 20*(1), 19–28.

Goldstein, A. (2002, March 22). Medical privacy changes proposed. *The Washington Post*, p. A-01.

Griffith, T. L. (1993). Teaching Big Brother to be a team player: Computer monitoring and quality. *Academy of Management Executive, 7*(1), 73–80.

Idehen, E. E. (1997). The influence of gender and space sharing history on the conceptions of privacy by undergraduates. *IFE-Psychologia, 5*(1), 59–75.

Ingham, R. (1978). Privacy and psychology. In J. B. Young (Ed.), *Privacy* (pp. 35–57). Chichester, UK: Wiley.

Iwata, O. (1988). Similarities and dissimilarities in the Japanese semantic structure of privacy and its associated concepts. *Psychologia, 31*, 198–206.

Jennings, C., & Fena, L. (2000). *The hundredth window: Protecting your privacy and security in the age of the Internet*. New York: The Free Press.

Johnson, C. A. (1974). Privacy as personal control. In D. H. Carson (Series Ed.) & S. T. Margulis (Vol. Ed.), *Man-environment interactions: Evaluations and applications: Part 2*, *Vol. 6. Privacy* (pp. 83–100). Washington, DC: Environmental Design Research Association.

Kagehiro, D. K. (1990). Psychological research on the Fourth Amendment. *Psychological Science, 1*(3), 187–193.

Kelvin, P. (1973). A social-psychological examination of privacy. *British Journal of Social and Clinical Psychology, 12*, 248–261.

Kinder, D. R. (1998). Opinion and action in the realm of politics. In D. T. Gilbert, S. T. Fiske, & G. Lindzey (Eds.), *The handbook of social psychology* (4th ed., Vol. 2, pp. 778–867). Boston: McGraw-Hill.

Klopfer, P. H., & Rubenstein, D. I. (1977). The concept *privacy* and its biological basis. *Journal of Social Issues, 33*(3), 52–65.

Krämer, B. (1995). Classification of generic places: Explorations with implications for evaluation. *Journal of Environmental Psychology, 15*(1), 3–22.

Krebs, J. R., & Davies, N. B. (1993). *An introduction to behavioural ecology* (3rd ed.). Oxford, UK: Blackwell Scientific Publications.

Larson, E. (1992). *The naked consumer: How our private lives become public commodities*. New York: Penguin.

Leary, M. R., & Schreindorfer, L. S. (1998). The stigmatization of HIV and AIDS: Rubbing salt in the wound. In V. J. Derlega, & A. P. Barbee (Eds.), *HIV & social interaction* (pp. 12–29). Thousand Oaks, CA: Sage Publications.

Linowes, D. (1996). *A research survey of privacy in the workplace*. Urbana, IL: The University of Illinois.

Louis Harris & Associates Polls. (2000). Public opinion poll database. Retrieved January 2000 from http://www.irss.unc.edu/data_archive

Lyon, D., & Zureik, E. (1996). Surveillance, privacy, and the new technology. In D. Lyon & E. Zuriek (Eds.), *Computers, surveillance, and privacy* (pp. 1–18). Minneapolis, MN: University of Minnesota Press.

Margulis, S. T. (1977). Conceptions of privacy: Current status and next steps. *Journal of Social Issues, 33*(3), 5–21.

Margulis, S. T. (1979). *Privacy as information management: A social psychological and environmental framework* (NBSIR 79-1793). Washington, DC: U.S. Department of Commerce, National Bureau of Standards.

Marx, G. T. (1984). Role models and role distance: A remembrance of Erving Goffman. *Theory and Society, 13*, 649–662.

Marx, G. T. (1999). Ethics for the new surveillance. In C. J. Bennett & R. A. Grant (Eds.), *Visions of privacy: Policy choices for the digital age* (pp. 39–67). Toronto, Ontario, Canada: University of Toronto Press.

McWhirter, D. A. (1994). *Search, seizure, and privacy*. Phoenix: Oryx Press.

Moore, B., Jr. (1984). *Privacy: Studies in social and cultural history*. Armonk, NY: Sharpe.

Murry, W. D., Wimbush, J. C., & Dalton, D. R. (2001). Genetic screening in the workplace: Legislative and ethical implications. *Journal of Business Ethics, 29*(4, part 2), 365–378.

Newell, P. B. (1998). A cross-cultural comparison of privacy definitions and functions: A systems approach. *Journal of Environmental Psychology, 18*, 357–371.

Nucci, L. (1997). Culture, universals, and the personal. *New Directions for Child Development, 76*, 5–22.

Regan, P. M. (1995). *Legislating privacy: Technology, social values, and public policy*. Chapel Hill, NC: University of North Carolina Press.

Regan, P. M. (1996). Genetic testing and workplace surveillance: Implications for privacy. In D. Lyon & E. Zureik (Eds.), *Computers, surveillance, and privacy* (pp. 21–46). Minneapolis, MN: University of Minnesota Press.

Richelson, J. T. (1995). *A century of spies: Intelligence in the twentieth century*. New York: Oxford University Press.

Rothstein, M. A. (Ed.). (1997a). *Genetic secrets: Protecting privacy and confidentiality in the genetic era*. New Haven, CT: Yale University Press.

Rothstein, M. A. (1997b). The law of medical and genetic privacy in the workplace. In M. A. Rothstein (Ed.), *Genetic secrets: Protecting privacy and confidentiality in the genetic era* (pp. 281–298). New Haven, CT: Yale University Press.

Rule, J., & Hunter, L. (1999). Toward property rights in personal data. In C. J. Bennett & R. Grant (Eds.), *Visions of privacy: Policy choices for the digital age* (pp. 168–181). Toronto, Ontario, Canada: University of Toronto Press.

Shaw, M. E., & Costanzo, P. R. (1970). *Theories of social psychology*. New York: McGraw-Hill.

Singleton, S. (1998). *Privacy as censorhip: A skeptical view of proposals to regulate privacy in the private sector* (Policy Analysis No. 295.). Washington, DC: The Cato Institute.

Stevens, J. (2001). *Good morning*. Allendale, MI: Grand Valley State University.

Stone, D. L., & Stone-Romero, E. F. (1998). A multiple stakeholder model of privacy in organizations. In M. Schminke (Ed.), *Managerial ethics: Moral management of people and processes* (pp. 35–59). Mahwah, NJ: Erlbaum.

Stone, E. F., & Stone, D. L. (1990). Privacy in organizations: Theoretical issues, research findings, and protection mechanisms. *Research in Personnel and Human Resource Management, 8*, 349–411.

Triandis, H. C. (1995). *Individualism and collectivism.* Boulder, CO: Westview Press.

U.S. Department of Health and Human Services. (2002, August 14). Standards for Privacy of Individually Identifiable Health Information: Final Rule. *Federal Register*, 45 CFR Parts 160 and 164, pp. 53181–53273.

USA PATRIOT Act of 2001, Pub. L. No. 107-56, 115 Stat. 272 (2001).

Warren, C., & Laslett, B. (1977). Privacy and secrecy: A conceptual comparison. *Journal of Social Issues, 33*(3), 43–51.

Weary, G., Gleicher, F., & Marsh, K. L. (Eds.). (1993). *Control motivation and social cognition*. New York: Springer-Verlag.

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

Wolfe, M., & Laufer, R. S. (1974). The concept of privacy in childhood and adolescence. In D. H. Carson (Series Ed.) & S. T. Margulis (Vol. Ed.), *Man-environment interactions: Evaluations and applications: Part 2, Vol. 6. Privacy* (pp. 29–54). Washington, DC: Environmental Design Research Association.

STEPHEN T. MARGULIS earned his doctorate in social psychology from the University of Minnesota. He taught in the Department of Psychology, University of Florida, was an applied environmental psychologist at the National Bureau of Standards, and then was Director of Research at BOSTI, an environmental design research and consulting firm. Since 1986, he has been Eugene Eppinger Professor of Facilities Management and later Professor of Management in the Seidman School of Business, Grand Valley State University. He served on the Boards of Directors of the Environmental Design Research Association and the International Facility Management Association. He co-authored the award-winning *Using Office Design to Increase Productivity* (Brill, Margulis, Konar, and BOSTI) and the well-received *Self Disclosure* (Derlega, Metts, Petronio, and Margulis). He edited the 1977 *Journal of Social Issues* issue “Privacy as a Behavioral Phenomenon.”