

MIS Quarterly

ISSUES AND OPINIONS

# HOW ETHICS CAN ENHANCE ORGANIZATIONAL PRIVACY: LESSONS FROM THE CHOICEPOINT AND TJX DATA BREACHES[1]

By: **Mary J. Culnan**
**IPM Department**
**Bentley University**
**175 Forest Street**
**Waltham, MA 02452**
**U.S.A.**
**mculnan@bentley.edu**

**Cynthia Clark Williams**
**Management Department**
**Bentley University**
**175 Forest Street**
**Waltham, MA 02452**
**U.S.A.**
**ccwilliams@bentley.edu**

## Abstract

*Protecting the privacy of personal information continues to pose significant challenges for organizations. Because consumers are vulnerable in their dealings with businesses due to a lack of information about and an inability to control the subsequent use of their personal information, we argue that organizations have a moral responsibility to these individuals to avoid causing harm and to take reasonable precautions toward that end. We further argue that firms can enhance their privacy programs by moving beyond merely complying with laws and other regulations and creating a culture of integrity that combines a concern for the law with an emphasis on managerial responsibility for the firm's organizational privacy behaviors. We use two high-profile data breaches experienced by two U.S. companies, ChoicePoint and TJX, to illustrate our arguments for enhancing organizational level privacy programs based on ethical reasoning. In doing so, this paper contributes to the dearth of prior organizational-level privacy research, which has largely overlooked ethical issues or the personal harms often caused by privacy violations. We conclude with recommendations for ways organizations can improve their privacy programs by incorporating moral responsibility.*

**Keywords**: Organizational privacy, information ethics, moral responsibility, information risk management, information management practices

## Introduction

Information privacy is an important information management issue that continues to challenge organizations. Previously, some privacy research focused on the problems resulting from the decisions organizations make about using or reusing personal information (e.g., Greenaway and Chan 2005; Smith 1993). Today, the decentralized technology environment contributes to a different organizational privacy problem: data breaches (Culnan et al. 2008). Breaches present a fruitful area for organizational privacy research because the United States is currently alone in requiring formal notice in the event of a breach (Schwartz 2009). The U.S. breach laws have resulted in a rich body of public information about breaches that currently does not exist elsewhere since without

[1]Detmar Straub was the accepting senior editor for this paper.

Both authors contributed equally.

notification laws, breaches remain private. Hence, we focus here on two large U.S. breaches which we use to illustrate our arguments.

We argue that integrating ethical reasoning into organizational privacy programs, specifically the moral responsibility[2] of "do no harm," will not only strengthen these programs, particularly with regard to breaches, but is increasingly necessary given the challenges of complying with the current legal requirements. We further argue that because consumers are vulnerable in their dealings with businesses due to information and control deficits, organizations have a moral duty—often overlooked, we observe—that extends beyond legal compliance requiring them to take reasonable precautions with consumer data and to avoid harm in using this data. Moral responsibility in this sense refers to causing, or helping to cause, an event to happen or, accordingly, by failing to prevent an event through omission (Velasquez 2003). Our arguments are both based on and extend the prior work in information ethics which recognizes that ethical quandaries involving information systems are often faced by decision-makers who are employed in corporate settings (see Mason et al. 1995; Smith and Hasnas 1999). It should be noted that this position, while not always leading to the highest profits, is both consistent with the profit motive of business and the moral responsibility of executives to do no harm.[3] By attributing the responsibility to executives within the firm, the related consequences or punishments are likely to be more just (Velasquez 2003), which may help improve information management practices and accountability (Weitzner et al. 2008), a main focus of the present paper.

Our paper is organized as follows. We begin by providing a conceptual overview of privacy, drawing on prior organizational privacy research. Next, we provide an overview of the regulatory environment in the United States governing personal data access and use, particularly as it relates to unauthorized access. Third, we describe the two high-profile data breaches at ChoicePoint and TJX to illustrate our arguments. Fourth, we argue why companies have a moral responsibility to the individuals who have provided their personal information, whether the information was acquired directly from individuals, or indirectly from third parties as in the case of commercial information providers. We conclude by offering recommendations for ways organizations can integrate moral responsibility into their information privacy programs.[4]

## The Concept of Privacy

Information privacy is a multidimensional concept that is dependent on context and also varies with a person's life experiences (Xu et al. 2008). It also suffers from definitional ambiguity (Solove 2006). Consistent with prior research on organizational privacy (e.g., Greenaway and Chan 2005; Smith 1993), we focus here on personal information generated by consumer transactions, and the privacy problems resulting from the subsequent storage, analysis, use, or sharing of this information.

Most research on privacy has not addressed broader organizational, managerial, and social issues such as how firms treat personally identifiable information, what managers are required to do, and the moral duties they have to various parties engaged in business with their companies. Prior research found that rather than being proactive and guided by internally agreed upon moral principles, organizations' privacy behaviors were largely reactive and driven by external pressures (Goodhue and Straub 1991; Greenaway and Chan 2005; Smith1993). For example, Smith's (1993) study found a consistent pattern of policymaking across financial service firms handling sensitive personal information that reflected a cycle of "drift–threat–reaction." Firms drifted with policy controlled primarily by middle managers until the organization perceived an external threat. At this point, senior executives became involved in developing the organization's "official" reaction to the threat. Similar results were reported by Straub (1990). When ethical theories are used to support the societal importance of these behaviors, they are often underdeveloped (Greenaway and Chan 2005). As Solove (2007a) points out, there is social value in ensuring that companies adhere to established limits on the way they use information to avoid violating personal and professional trust.

[2]The term *duty* has been used to refer to what one ought to do (DeGeorge 2006; Velasquez 2003) and since we are concerned with both descriptive and normative aspects of morality, we will use the terms *duty* and *responsibility* interchangeably. In a slightly different vein, the term *obligation* is often used to express a strong duty often associated with a contractual duty (Raz 2003) and thus we are not focusing on moral obligations in this paper.

[3]This responsibility is typically considered a *prima facie* duty in that it can be overridden by other duties. For example, unless stronger moral considerations override it, one ought to keep promises made and contracts entered into.

[4]After Greenaway and Chan (2005), we define *organizational privacy behaviors* as how firms treat individuals' personal information and *information privacy programs* as the collection of policies and procedures organizations implement to manage the collection, use, reuse, security, and disposal of personal information.

Prior organizational research on privacy has also typically defined information privacy from the perspectives of individuals in terms of their ability to control or limit access to their personal information (see Xu et. al. 2008). Alternatively, Solove (2006) characterized privacy as a set of problems arising from the ways organizations process personal information. He developed a taxonomy of information processing and information dissemination activities that have the potential to result in harm to individuals, resulting in privacy problems. For the purposes of this paper, most of these activities may be grouped into two broad categories: *information reuse* and *unauthorized access to personal information*.[5] Typically, information reuse involves organizations making legal decisions about new uses for the personal information they have collected, while unauthorized access represents activities that violate either laws or corporate policies. Both activities, information reuse and unauthorized access, can potentially threaten an individual's ability to maintain a condition of limited access to his/her personal information, harm individuals, and subsequently threaten the organization's legitimacy in its interactions with consumers, shareholders, and regulators (Greenaway and Chan 2005; Smith 1993; Solove 2006). Figure 1 illustrates these two types of activities and the potential harms that can result from each.

Unauthorized access, the second type of privacy problem, includes two types of activities: browsing and data breaches. In the case of browsing, employees view personal information they are not authorized to view as in the case of individuals who browse a celebrity's records. Breaches involve unauthorized access to personal information, resulting from a variety of security incidents including hackers breaking into systems or networks, third parties accessing personal information on lost laptops or other mobile devices, or organizations failing to dispose of personal information securely. Privacy harms resulting from unauthorized access can include a breach of confidentiality and trust, or the financial harm to individuals from identity theft or identity fraud. In this paper, we focus on the privacy issues resulting from unauthorized access, specifically data breaches, for reasons we will describe subsequently.

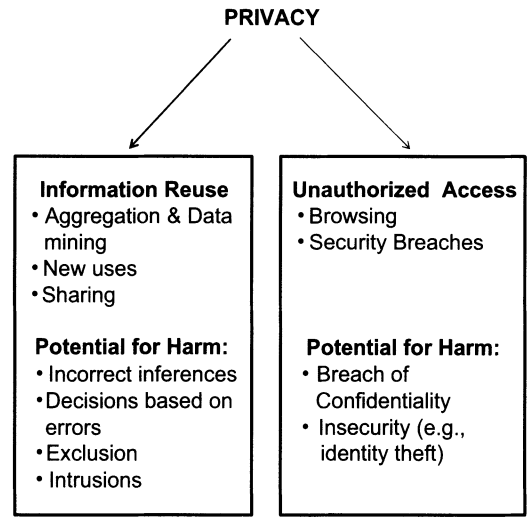
[5]Consistent with Solove, we define *security* as one aspect of privacy. However, privacy includes more than security as Figure 1 illustrates. Security is about protecting personal information, while privacy is broader and encompasses permission and use of personal information. Privacy is difficult to achieve without security. However, organizations can successfully secure the personal information in their custody and still make bad decisions about how the personal information they have collected is subsequently used, resulting in a privacy problem. Further, fair information principles (which we describe subsequently) state that organizations have a responsibility to secure personal information from unauthorized access (see Table 1).

## The Privacy Legal and Regulatory Landscape

Fair information practices (FIPs) are the prevailing global data protection principles that address privacy harms by defining guidelines for individual rights and organizational responsibilities, thereby reflecting social expectations for responsible information use (Culnan and Bies 2003; Greenaway and Chan 2005; Smith 1993). They attempt to balance some of the competing business and individual interests with legitimate uses of personal information and serve as the basis for privacy laws and industry self-regulatory programs in the United States and elsewhere. Therefore, FIP's provide guidance to organizations about socially responsible privacy behaviors while their adoption provides an evaluation tool for external audiences on the organization's degree of responsiveness (Smith 1993). The American Institute of Certified Public Accountants and the Canadian Institute of Chartered Accountants recently released the Generally Accepted Privacy Principles (GAPP), which is a current example of a comprehensive implementation of FIP (AICPA/CICA 2006). Table 1 contains a summary of the GAPP.

While there is consensus in principle that fair information practices constitute socially responsible information practices, there is no consensus about how the individual principles should be implemented. In most of the world, fair information practices are implemented through omnibus laws. However, in the United States there are no comprehensive laws requiring *all* organizations to observe fair information practices. Instead, the United States has adopted a sectoral approach to regulating privacy where laws are typically enacted in response to a specific problem within a single industry. As a result, both the operationalization and implementation of the FIP principles in the United States is uneven. Further, the typical U.S. implementation of FIP also reflects only a subset of the principles: notice, choice, access, security, and sanctions for noncompliance (Culnan and Bies 2003). Table 2 summarizes the requirements of four major U.S. laws, one state law, and one industry standard: the Fair Credit Reporting Act (FCRA), the Gramm-Leach-Bliley Act (GLBA), the privacy regulations of the Health Insurance Portability and Accountability Act (HIPAA), Section 5 of the Federal Trade Commission Act, the Massachusetts Security Rule,[6] and the Payment Card Industry Data Security Standard (PCI-DSS) (Majoras 2005; Schwartz and Solove 2008; Smedinghoff 2008; Smedinghoff and Hamady 2008).

[6]The Massachusetts Security Rule has national reach as it applies to any organization maintaining personal information on a Massachusetts resident, independent of where the organization is located.




Adapted from Smith (1993) and Solove (2006)

Figure 1. Two Faces of Privacy Problems

Table 1. AICPA/CICA Generally Accepted Privacy Principles

| Principle | Definition |
|---|---|
| 1. Management | This principle requires the organization to define, document, communicate, and assign accountability for its privacy policies and procedures. |
| 2. Notice | This principle requires the organization to provide notice about its privacy policies and procedures. This includes the purpose(s) for which personal information is collected, used, retained, and disclosed. |
| 3. Choice and Consent | This principle requires the organization to describe the choices available to the individual related to the use and disclosure of their information, and to obtain implicit or explicit consent with respect to the collection, use, and disclosure of personal information. |
| 4. Collection | This principle requires that the organization collect personal information only for the purposes identified in the notice. |
| 5. Use and Retention | This principle requires that the organization limits the use of personal information to the purpose(s) identified in the notice and/or for which the individual has provided implicit or explicit consent. |
| 6. Access | This principle requires that the organization provides individuals with access to their personal information for review and correction. |
| 7. Disclosure to Third Parties | This principle requires that the organization discloses personal information to third parties only for the purposes identified in the notice and only with the implicit or explicit consent of the individual (unless disclosure is required by law). |
| 8. Security for Privacy | This principle requires that the organization protects personal information against unauthorized access (both physical and logical). |
| 9. Quality | This principle requires that the organization maintain accurate, complete, and relevant personal information for the purposes identified in the notice. |
| 10. Monitoring and Enforcement | This principle requires that the organization monitors compliance with its privacy policies and procedures, and have procedures to address privacy-related inquiries and disputes. |

Source: AICPA/CICA (2006)

**Table 2. Privacy Provisions of Key Laws and Industry Standards**

| Law/Standard | Who Is Covered | Requirements |
|---|---|---|
| Fair Credit Reporting Act (FCRA) | Consumer reporting agencies | Personal information in a consumer report may only be disclosed for a permissible purpose (e.g., credit, insurance underwriting, employment, or other transaction initiated by the consumer). Individuals have the right to access their consumer reports and to correct errors. |
| Gramm-Leach-Bliley Act (GLBA) | Financial institutions | Insure the security and confidentiality of customer records and information, protect against any anticipated threats or hazards to the security or integrity of records, and protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer. Also requires an annual privacy notice to customers and limits sharing of nonpublic personal information with unaffiliated third parties. |
| Health Insurance Portability and Accountability Act Regulations (HIPAA) | Health organizations that exchange treatment, payment, or operations information in a standard electronic format | Covered entities must implement policies and procedures to prevent, detect, contain, and correct security violations. Requirements include implementing a comprehensive risk management program, workforce security, information access management, security awareness, and training. Requires privacy notices to patients and restricts dissemination of personal information for purposes other than treatment, payment, or operations. |
| Section 5 of the Federal Trade Commission Act | All commercial organizations over which the FTC has jurisdiction | Prohibits unfair or deceptive acts or practices. Failure to implement reasonable security may constitute an unfair trade practice if a breach results in harm to consumers that could not reasonably be avoided by the individual and which could be reasonably avoided by the firm. Firms may also be prosecuted for making a false statement in their privacy policy. |
| Massachusetts Security Rule (201 CFM 17.00) | All individuals or organizations that maintain personal information on a Massachusetts resident | Develop, implement, maintain, and monitor a comprehensive written information security plan that is consistent with industry standards. Implement administrative, technical, and physical safeguards. Includes both electronic and paper records. |
| Payment Card Industry– Data Security Standard (PCI–DSS) | Organizations accepting credit or other payment cards | Implement an information security policy, build and maintain a secure network, maintain a vulnerability management program, implement strong access control measures, regularly monitor and test networks. |

Source: Schwartz and Solove (2008), Smedinghoff and Hamady (2008), and Payment Card Industry Security Standards Council (2006), *About the PCI Data Security Standard (PCI DSS)* (available at https://www.pcisecuritystandards.org/security_standards/pci_dss.shtml).

As a result, for organizations that collect, maintain, and use personal data, the laws governing these practices impose requirements that are unclear or may vary across jurisdictions or types of data, thereby posing difficult compliance challenges. These challenges may be further exacerbated by conflicts in the requirements of multiple state laws (Zeller 2005). An overarching sentiment in most of these statutory laws and regulations is to recognize a duty of care among these organizations regarding the data they collect and maintain based on the consumer's vulnerability and the real potential for harm (Smedinghoff 2008; Solove 2007a). For example, the FCRA limits the use of consumer reports provided by commercial information providers to "permissible purposes," and provides individuals with the right to access their reports and correct errors. The requirements imposed by GLBA technically apply only to financial institutions as defined in the law. Likewise, both GLBA and HIPAA limit certain uses of personal information and require covered organizations to provide notice to consumers. GLBA, HIPAA, the Massachusetts Security Rule, and the PCI-DSS standard require that organizations implement process-based formal information security programs that meet

certain standards. Finally, the courts have begun to recognize that all companies have a responsibility under common law to protect the personal information in their custody including both preventing unauthorized access and sharing information with third parties when there is a foreseeable risk of harm (Smedinghoff 2008; Solove 2007b).

Although compliance with government regulation leads to organizational legitimacy—or the acceptance of an organization by its external environment (DiMaggio and Powell 1983; Meyer and Rowan 1977)—it is often challenging to achieve. For example, organizations are judged to be in compliance with the current security requirements if they maintain "reasonable procedures" (Lee and Mudge 2006; Solove et al. 2006). However, the prevailing regulations are not specific about what constitutes *reasonable* or *appropriate*, which varies according to the nature and size of the organization, the types of information it has, the security tools available based on the organization's resources, and the risks the organization is likely to face (Lee and Mudge 2006; Smedinghoff 2008), making compliance less straightforward.

Likewise, critics have long argued that existing laws are often reactive and outdated by the time they are enacted (DeGeorge 2006; Smith and Hasnas 1999; Stone 1975) and that violations of most privacy laws are detected and prosecuted only based on a required disclosure or a complaint filed *after* a violation has occurred and the damage is done (Mason et al. 1995; Solove 2006; Stone 1975). For all of these reasons, neither laws nor lawsuits have proven adequate in protecting consumers (Baker et al. 2008, Mason et al. 1995; Stone 1975).

## Data Breaches as a Privacy Problem ■

Still, consumers face a variety of privacy problems and each varies in terms of the level of harm they pose. Here, we focus on one type of privacy problem, data breaches resulting from unauthorized access. However, we believe our overall conclusions can be applied to enhancing organizational privacy programs in general, and are not limited solely to addressing the problem of data breaches. We have selected data breaches for four reasons. First, they are becoming highly visible due to the recent breach notification laws in the United States. Second, unlike some other privacy problems, breaches cause tangible harm to both organizations and individuals. Third, despite laws and regulations requiring most organizations to implement comprehensive security programs, breaches continue to occur, suggesting that existing compliance programs are not effective. Fourth, there is the potential that breaches may also lead to spillover effects for other firms in the same industry when they serve as a catalyst for new government regulation (Yu et al. 2008).

The Privacy Rights Clearinghouse reported that since January 2005, more than 246 million records containing sensitive personal information have been exposed due to data breaches. While breaches are in the headlines today, they are not a new phenomenon (see Goodhue and Straub 1991; Straub 1990; Straub and Welke 1998). What is noteworthy is that a recent spate of state laws in the United States require affected organizations to provide notice if they suffer a breach meeting certain criteria. California passed the first breach notification law which took effect in 2003. Subsequently, more than 40 states have enacted similar laws requiring organizations to notify affected individuals and regulators when they experience a data breach as defined by these laws. As a result, the public is now aware of breaches occurring in the United States and the information is now accessible to researchers.[7]

A recent analysis by Verizon Business of more than 500 forensic investigations of U.S. breaches involving more than 230 million records found that nearly 90 percent could have been prevented had reasonable security measures been implemented. Nine out of 10 of the breaches involved a system that was unknown to the organization or had unknown network connections or accessibility, or a system that stored data that the organization did not know existed on that system. Further, patches had been available for at least six months prior to the breach for 90 percent of known vulnerabilities exploited by these attacks. In the majority of cases, organizations had failed to implement standard security policies and procedures and were slow to detect most breaches. In fact, rather than detecting the breach themselves, 70 percent of the firms in the study learned they had suffered a breach from a third party (Baker et al. 2008). Even though Smith (1993) found that all of the companies in his study had formalized information security policies, many of the policies were somewhat outdated and subject to lapses in implementation. The results of the recent Verizon study (Baker et al. 2008), however, suggest that little has changed since Smith's research. We now briefly describe the two breaches we use to illustrate our arguments.

[7]Clearly data breaches are not unique to the United States and most countries including the United States have enacted data security laws (Smedinghoff 2008). However, while the European Union and other countries are currently considering adopting breach notification laws, the United States is currently alone in requiring notice in the event of a breach (Schwartz 2009).

## Overview of Two Breaches: ChoicePoint and TJX

### ChoicePoint Inc.

ChoicePoint provides a wide range of credentialing, background screening, authentication and public records services to businesses, nonprofit organizations, and government agencies. Its services are based largely on personal information acquired from third parties rather than being acquired directly from individuals. Founded in 1997 as a spin-off from Equifax, one of the three major U.S. credit bureaus, ChoicePoint originally provided data to the insurance industry. Subsequently, ChoicePoint has grown to include five business segments: insurance services, screening and authentication services, financial and professional services, government services, and marketing services. Approximately 60 percent of ChoicePoint's business is driven by transactions initiated by consumers such as preemployment screening or insurance underwriting and the majority of these transactions are regulated by the FCRA (Curling 2005; Williams 2008). In February 2008, ChoicePoint was acquired by Reed Elsevier. The cash transaction was valued at $3.6 billion.

In February 2005, ChoicePoint sent letters to 145,000 individuals notifying them that, during 2004, their personal information had been fraudulently accessed and used to commit identity theft. The breach resulted from failures in ChoicePoint's credentialing procedures for new subscribers. As a result, criminals masquerading as small businesses were provided customer accounts and these individuals subsequently made fraudulent use of the data, in violation of the Fair Credit Reporting Act. This breach was not the first time ChoicePoint experienced a failure in its credentialing procedures; as early as 2000, identity thieves used fake documents to pose as legitimate customers (Bureau of National Affairs 2005). Table 3 contains further information about the ChoicePoint breach, including additional details about the cause of the breach, parties affected by the breach, and ChoicePoint's response.

### TJX Companies, Inc.

TJX is an off-price retailer operating eight businesses and over 2,400 stores in the United States, Puerto Rico, Canada, and Europe. Its stores include T. J. Maxx, Marshalls, HomeGoods, A. J. Wright, and Bob's. TJX collected and stored customer information to authorize payment card purchases, authorize personal checks, and process merchandise returned without a receipt, in violation of industry standards prohibiting the retention of the most sensitive information from the magnetic strip on a credit card (Aplin 2007).

In January 2007, TJX issued a press release and filed a Form 8-K disclosure statement with the Securities and Exchange Commission stating that it had suffered a systems intrusion detected in December 2006 (Bureau of National Affairs 2007a). Beginning in 2005, criminals breached TJX's networks and stole customer payment information on more than 45 million consumers over an 18 month period (Pereira 2007). TJX was faulted for storing unencrypted sensitive information, for failing to limit unauthorized wireless access to their networks, and for failing to employ appropriate security measures on its networks (Federal Trade Commission 2008). Table 3 also contains additional information about the TJX breach. We now turn to a discussion of moral responsibilities of firms with regard to information privacy.

## Moral Responsibilities

Normative theories of ethics refer to what an individual or groups of individuals *ought* to do so as to provide basic moral principles from which norms can be derived. While business ethics is the study of the interaction of ethics and business, information ethics concerns itself more specifically with ethical dilemmas arising from the collection, use, and management of information (Mason 1986). Four areas of concern critical to this intersection were identified by Mason (1986): privacy (what personal information should individuals be required to disclose and under what conditions), accuracy (what policies and standards are needed to protect individuals from errors), property (who owns data and how should ownership be determined), and access (who can have access to what information). As technologies have become more complex and established within society, ethical problems associated with these issues have tended to increase (Moore 2005); however, the theories to address these challenges remain underdeveloped (Greenaway and Chan 2005). Given the large social impact of privacy problems in general and data breaches in particular, two aspects of morality are central to the relationship between those who collect and use personal information and the individuals who provide their information: vulnerability and avoiding harm.

### Vulnerability

Vulnerability explains many of our widely held moral intuitions. It exists where one party in a relationship is at a disadvantage with regard to the other. Typically, this situation

Table 3. Summary of ChoicePoint and TJX Breaches

| Attribute | ChoicePoint | TJX |
|---|---|---|
| Company overview | Data broker selling information for identifying and verifying credentials of individuals to businesses, governments, and others. Information typically used for preemployment screening and insurance underwriting. | Off-price retailer operating eight businesses and over 2,400 stores worldwide including T. J. Maxx, Marshalls, HomeGoods, and A. J. Wright. |
| How personal information was acquired | ChoicePoint obtained data from a wide range of third-party sources including insurance claims data, public records, motor vehicle records, and credit reports. Information typically collected without any direct contact with individual. | Customer provided information during sales transactions. |
| Date breach made public | February 2005. | January 2007. |
| Cause of breach | **Organizational Process**. ChoicePoint provided customer accounts to criminals and failed to maintain reasonable procedures for credentialing new subscribers and ensuring permissible uses of the data. ChoicePoint accepted documentation that called into question the reliability of the information supplied by the applicant or contained contradictory or illogical application information. | **Technological**. Criminals connected to TJX's networks and stole customer payment information. TJX failed to implement reasonable information security procedures including storing and transmitting sensitive information as clear text, failed to limit wireless access to its networks, failed to detect or prevent unauthorized access to computer networks or to follow up on security warnings and intrusion alerts. |
| Scope of breach | At least 145,000 consumer reports accessed fraudulently. | At least 46.2 million credit cards over an 18 month period. |
| U.S. laws violated | • Fair Credit Reporting Act (FCRA): Sold consumer reports for impermissible purposes; failed to maintain reasonable procedures to limit furnishing of consumer reports for permissible purposes specified by law.<br>• FTC Act: *Unfair practices* that resulted in substantial harm to consumers that could not be avoided and *deception* as Choice Point misrepresented some of its security procedures in consumer publications. | • FTC Act: Unfair practice that resulted in substantial harm to consumers that could not be avoided.<br>• TJX was also found not to be in compliance with payment card industry (PCI) security standards. |
| Who was affected | **ChoicePoint** costs estimated at $30 million including fines of $10 million plus $5 million to create a fund for consumer redress. Required to undergo biennial independent assessments for 20 years and provide copies to FTC upon request.<br>**Individuals** whose identity was stolen and used fraudulently.<br>**Other businesses** as ChoicePoint restricted the types of information it would sell and the types of customers it would serve going forward. | **TJX** costs estimated could reach $156 million including $40.9 million to Visa and $24 million to MasterCard to cover fraud losses. FTC Consent Agreement requires TJX to implement a comprehensive information security program and to undergo biennial independent assessments for 20 years and provide copies to the FTC upon request.<br>**Consumers** whose identity was used fraudulently.<br>**Banks and credit card companies** who replaced payment cards.<br>**Other businesses** who experienced fraudulent transactions using stolen identities. |

**Table 3. Summary of ChoicePoint and TJX Breaches (Continued)**

| Attribute | ChoicePoint | TJX |
|---|---|---|
| Company response following breach | • Hired Ernst & Young to help redesign its procsses.<br>• Hired a Chief Credentialing, Compliance and Privacy Officer (CCPO) reporting to Board of Directors.<br>• Created Consumer Advocacy Office.<br>• Implemented mandatory employee training program.<br>• Exited lines of business posing unacceptable levels of risk. Limited types of customers it will accept as subscribers and types of products it will sell going forward.<br>• Truncated or removed certain sensitive data.<br>• Instituted random daily customer audits.<br>• CEO to be notified of all incidents when detected.<br>• Adopted new controls based on AICPA GAPP.<br>• Completed over 100 third-party audits. | • Hired security consultants and strengthened the security of its systems.<br>• Became PCI compliant, which requires the following ongoing measures:<br>– Maintaining an information security policy<br>– Building and maintaining a secure network<br>– Protecting cardholder data<br>– Maintaining a vulnerability management program<br>– Implementing strong access control measures<br>– Regularly monitoring and testing networks<br>• Recruited for at least two new IT security positions. |

Source: FTC (2006; 2008) with additional reporting by *BNA Privacy & Security Law Report*. ChoicePoint examples are further based on public information including case analyses, press releases, media reports, and information posted by ChoicePoint on its website (www.choicepoint.com). In particular, see ChoicePoint (2008), Litan (2006), Rivlin (2006), and Williams (2008).

exists because the disadvantaged party suffers a deficit of information and control (Goodin 1985; Marcoux 2003).[8] Similarly, these are also the types of power imbalances that Solove (2007a) noted are at the root of large-scale privacy harms.

This vulnerability is often the result of the large amount of personal information that is gathered from consumers. As a result, the majority of consumer transactions consist of not one but two exchanges. First, consumers exchange money for products or services. There is a large amount of information to help consumers make informed decisions about this "first exchange," including product labels, prior experience, word-of-mouth or independent ratings, and reviews. Post-purchase, consumers' control how the product is used and their experience helps them to decide whether or not to be a repeat customer. However, today, the majority of consumer transactions also involve a "second exchange" where the consumer also provides personal information in exchange for something of value such as information, home delivery, the ability to use a credit card, personalized service, or discounts (Culnan and Milberg 1998). Inadvertently, the individual gives up control of the subsequent uses of their information. Privacy advocates have argued that in these types of exchanges consumers are justified in expecting that the information they share remains private among those to whom it was originally disclosed, rather than shared with third parties who may subsequently behave opportunistically (Petronio 2002). Even if a firm attempts to address these deficits by providing notice of its information practices at the time it collects personal information, the firm cannot anticipate all future uses that will be made of that information (DeGeorge 2006), making it more difficult to account for any new uses of information going forward (DeGeorge 2006; Introna and Pouloudi 1999). Yet, exercising reasonable care by attempting to protect the consumer's vulnerability is both germane to preventing potential unauthorized access and a more effective way to monitor the subsequent uses of information.

In the cases of both ChoicePoint and TJX, consumers were vulnerable. Individuals whose data ChoicePoint stored lacked knowledge about the risks posed by ChoicePoint's credentialing procedures and the ability to influence these procedures while also giving up control of the information they had originally disclosed to another organization which subse-

[8] Although Marcoux uses information vulnerability in the context of fiduciary duty, we are not arguing here that data providers have a fiduciary duty to individual consumers because data providers do not appear to fit the definition of a fiduciary in that they are not obligated, *primarily*, to advance the interests of another party, the beneficiary (Marcoux 2003, p. 3), or the individual consumer in this case. Instead, Marcoux argues that a firm's directors and officers have fiduciary duties only to shareholders over the project of directing the activities of the firm.

quently provided the information to ChoicePoint. In some cases, these consumers were not informed about these subsequent uses of their information either (Williams 2008). TJX's customers also suffered from similar vulnerabilities in that they had no knowledge of the misuse of their credit card data resulting from TJX's lax security measures and also lacked the influence or power to correct the problem. While these customers may have implicitly consented to TJX using the credit card data as payment for their purchases, it is also likely they expected TJX to protect their data after the fact.

Adding to the consumer privacy debate is the recognition that consumers benefit from various forms of data collection. Privacy provides individuals with relief from social friction, enabling activities that are socially worthwhile (Solove 2006). While privacy is important, it is not absolute and needs to be balanced against other important countervailing interests (Culnan and Bies 2003; Smith 1993; Solove 2006). To be sure, consumers need and want credit cards, loans, life insurance, and health care, for example. In order to offer these products, firms need personal information such as credit histories and medical information. Therefore, the individual's privacy—and the subsequent loss of some information and control—must be balanced against the rights and legitimate needs of others (Valesquez 2006). But, the question remains: How can managers achieve this balance?

## Avoiding Harm

While there exists some controversy regarding information privacy rights, most ethicists agree that managers have a minimum moral responsibility to do no harm in their treatment of information (DeGeorge 2006; Goodpaster 1987; Marcoux 2003; Valesquez 2003), especially when their treatment makes consumers unnecessarily vulnerable. A manager can strike a balance between the legitimate, competing consumer privacy and business interests by understanding and adhering to the principle of not causing harm to an individual in the process of using personal data that their company acquired.

In contrast, both the ChoicePoint and TJX breaches caused harm. At a minimum, the ChoicePoint breach caused harm to those whose sensitive data (e.g., name, address, date of birth, social security number) it allowed to fall into the hands of criminals. In both instances, the do no harm principle was violated. Moral responsibility was absent from these privacy behaviors as TJX and ChoicePoint caused harm to vulnerable individuals by failing to take reasonable efforts to avoid it. Specifically, TJX failed to prevent harm by violating industry rules about collecting and storing credit card data and then storing such data on an unsecured wireless server. Choice Point failed to take reasonable efforts to avoid harm, for example, by allowing lax credentialing even though it had credentialing policies in place. Both breaches harmed the individuals whose personal information was obtained illegally and used to commit identity fraud or identity theft. Therefore, in the relationship that exists between consumers and firms, a moral responsibility to do no harm cannot be independent of the organization's information privacy program because the deficits of information and control make the consumer vulnerable, and this vulnerability can result in harm to the consumer if the information is misused (DeGeorge 2006; Solove 2006, 2007a, 2007b).

It is also interesting to note that the two firms responded to their respective breaches, as a way of mitigating future harm, in very different ways as Table 3 illustrates. TJX brought its data security practices into compliance, while ChoicePoint addressed the weaknesses in its credentialing procedures. In this way, both companies acquiesced to institutional demands in order to regain acceptance by the external environment (DiMaggio and Powell 1983; Greenaway and Chan 2005; Scott 2003) in a fairly predictable *ad hoc* fashion. In our opinion, however, only ChoicePoint went beyond compliance and implemented both procedural and structural changes. We think that these differences may be attributed to the fact these two firms operate in very different industries. ChoicePoint's business is the sale of personal information. It operates in a highly regulated industry and responsible information practices are essential to its survival, perhaps giving the company added incentive to correct its errors more quickly and substantively. TJX's information practices are ancillary to its core business as a retailer and its actions suggest it took only the steps necessary to bring its practices in line with those expected in its industry.

## Ethics is Good Business

In its simplest terms, business activities, like other human activities, cannot exist unless people follow a minimum moral principle and this principle is consistent with business pursuits, such as making a profit. While there is an ethical argument for protecting consumers because they are vulnerable and because it is what a firm ought to do, there are also business reasons for doing so. First, problems resulting from a failure to protect consumer information can also, ultimately, threaten the fiduciary relationship with shareholders if a breach has a negative impact on the bottom line as a result of customer defections, fines, or other costs incurred in ad-

dressing a breach. Further, many of the same protections that secure customer information can also help to protect sensitive corporate information such as trade secrets and intellectual property as unauthorized access to this information can have significant financial consequences for the firm.

Second, a firm that recognizes its moral responsibilities is also likely to gain legitimacy in the eyes of important internal audiences like employees or the board of directors, and external audiences such as regulators, the media, and special interest groups such as privacy advocates. Organizations perceived as legitimate are better able to acquire resources necessary for the organization's survival and are more likely to be perceived as trustworthy (Porter and Kramer 2006; Suchman 1995). Therefore, a commitment to avoid harm is both ethical and prudent.

Government bodies and legislative actions are two types of external forces that confer legitimacy on an organization (DiMaggio and Powell 1983; Meyer and Rowan 1977). If a company is seen as conforming to these norms of behavior—enhanced internally through its moral responsibility—it is likely to garner not only necessary resources such as new contracts, loyal customers, or a license to operate but, with it, *moral* legitimacy: an external judgment that the organization's activities are the right thing to do in terms of promoting social welfare (Suchman 1995). Firms achieving moral legitimacy have, for example, a culture of integrity that combines legal compliance with an emphasis on managerial responsibility for the firm's ethical behavior (Paine 1994). These are firms that would make attempts to avoid causing harm in the first place and would hold themselves accountable.

Third, incidents experienced by a single firm can cause spillover effects with repercussions affecting an entire industry. This process is often fueled by external institutional intermediaries such as the media or regulators who influence the views of other stakeholders (Yu et al. 2008). For example, the ChoicePoint breach motivated Congress to hold hearings to investigate information practices in the data broker industry. Following the TJX breach, Massachusetts issued its 2008 security rule, which imposes stringent organizational and technical requirements on anyone who maintains personal information on Massachusetts residents, with other states expected to follow (Smedinghoff and Hamady 2008). Legislation was also introduced in several states to hold all retailers responsible for the costs incurred by banks in reissuing new credit cards to individuals whose credit card numbers had been stolen in a breach (Bureau of National Affairs 2007b). Spillover effects such as new regulations can also threaten an organization's legitimacy because they can cause other firms in the same industry to incur substantial new costs even though they were uninvolved in the original crisis.

Although ChoicePoint did lose customers (Williams 2008) and both companies incurred meaningful reputational damage, fines, and a requirement to submit to Federal Trade Commission monitoring of their compliance for 20 years (Kerber 2007; Pereira 2007; Williams 2008), the regulatory spillover effects for each industry and the potential costs of more regulation may convince some managers to conclude that they are, in fact, in the reputation business and the excuse that they complied with the law does nothing to build trust after the dam has broken. Therefore, we now turn to a discussion of specific implications for managers.

## Implications for Practice: What Should Managers Do?

In this section, we offer a set of best practices that organizations can adopt to improve their organizational privacy programs by incorporating moral responsibility. We advocate that organizations need to take three steps to develop robust privacy programs that will result in improved privacy behaviors: (1) create a culture of privacy that begins at the top of the organization, (2) create an accountable governance process for privacy, and (3) avoid decoupling privacy from personal experience.

### *Create a Culture of Privacy*

First, organizations need to create a culture of privacy that begins at the top. Increasingly, due to their fiduciary responsibilities, the duty of care for both CEOs and boards of directors includes responsibility for protecting both personal information and the organization's information systems (Smedinghoff 2008). Prior research found that top executives' values influence organizational outcomes because these executives possess the status necessary to influence vital organizational actions (Finklestein and Hambrick 1990), and as a result, managers will invest in ethics programs, policies, and structures in order to demonstrate their commitment to moral responsibility (Weaver et al. 1999a).

However, organizations have been slow to accept this responsibility. For example, the 2004 Ernst & Young Global Information Survey found that only 20 percent of the more than 1,200 organizations surveyed felt strongly that their organizations viewed information security as a CEO-level priority (Ernst & Young 2004). This finding was supported by the results of a recent survey of 703 members of boards of U.S. public companies, which found that a majority of members

are uninvolved in the types of activities that would constitute meaningful oversight of information privacy and failed to receive or review privacy and security risk policies or assessments (Power 2008).

As described previously, moral responsibility is driven from the top of the organization and privacy problems are more likely to occur when the CEO fails to set and articulate the appropriate tone, fails to provide active support for ethical practices (Weaver et al. 1999a), or fails to implement mechanisms to monitor and detect problems (Paine 1994; Smith 1993). Indeed, corporate misconduct is rarely explained by the flaws of a lone actor; rather, it reflects the values, attitudes, and behavior that characterize an organization's culture (Paine 1994). Lack of leadership continues to plague organizational privacy behaviors. For example, Smith (1993) found that the absence of leadership on privacy posed ethical dilemmas for employees who are responsible for the firm's privacy behaviors on a day-to-day basis. In the latest survey of key issues for IT executives, privacy and security dropped to number 6 in 2007 from number 3 in 2006, despite the visibility of data breaches and the increased risk resulting from the fact that organizations' value chains are increasingly linked electronically (Luftman and Kempaiah 2008). Perhaps these policies are viewed as mere "window dressing" as has been the case with other such compliance programs (Weaver et al. 1999b).

Robust privacy programs are both costly and difficult. Since there is no obvious return, the firm's risk calculations may not justify the costs involved in building a culture of integrity (Austin and Darcy 2003; Osterhus 1997). Therefore, it is unlikely an organization will succeed in moving from a compliance mind-set to a culture of integrity unless there is moral commitment from the CEO.

### Implement Governance Processes for Privacy

Organizations may incorrectly assume that legal compliance with privacy laws consists of a situation where appropriate controls have been implemented at a particular point in time. However, such a view presumes a static world. Instead, organizations need governance processes to ensure that their privacy behaviors comply with the law, and to also ensure that their privacy programs accurately reflect their current risk environment as well as their current information practices. Organizations can significantly enhance their privacy programs if they implement a comprehensive governance structure involving both the board and senior management, as well as employees who use and/or manage information. The recent recommendations issued by the CyLab at Carnegie Mellon University suggest that, in addition to establishing an ongoing process for privacy, organizations also need to establish a cross-organizational committee which meets regularly to coordinate and communicate on all types of privacy issues (Power 2008). The membership of this privacy committee should include senior management from all departments that either use or manage personal information, and the team should report regularly to the CEO and to the risk committee of the board.

This committee—similar to a disclosure committee as recommended by the Sarbanes-Oxley Act of 2002 (SOA)—should serve as a central decision-making body for issues of privacy. The main function of the privacy committee is to reduce risks and errors in managing personal information and to provide oversight for the organization's privacy programs. For example, the committee should review the organization's security program on an ongoing basis, ensure that it is consistent with best practices and that it addresses any identified weaknesses. The committee should also deliberate the myriad of issues surrounding the use of personal information and ensure that the organization's privacy behaviors conform to fair information practices including whether information gathered is directly relevant to the stated purpose or whether the consumer has been informed as to the intended purpose for which the information is being collected.

One way to address emerging organizational privacy issues prospectively in a systematic way is to conduct a privacy impact assessment (PIA) and have the privacy committee review the results. A PIA is a risk management tool used to ensure that any *new* systems or *new* uses of personal information comply with legal requirements, to determine the risks of collecting and using personal information, and to assess protections and alternative methods of processing to mitigate privacy risks *before* the new application is developed (U.S. OMB 2003). The goal of a PIA is to ensure that the organization's practices are consistent with fair information practices regarding what information is collected and how it will be used, ensure data quality, and ensure that appropriate controls are implemented to avoid unauthorized access. The E-Government Act of 2002 mandates that U.S. federal agencies conduct a PIA before developing any new electronic information systems and make the results of the PIA available to the public.

A privacy committee would also be instrumental in enhancing the organization's internal controls, as mandated by SOA section 404. Likewise, through this structural change, an organization can establish a set of procedures that are socially acceptable, and gain moral legitimacy by demonstrating that it is making a good faith effort toward achieving meaningful

ends (Scott 2003). These governance procedures are also seen as having positive moral value in and of themselves (Berger et al. 1973).

The need for such governance is obvious. In both prior research and in media reports of a range of privacy events including the two high profile cases we described in this article, it is clear that when a privacy crisis hits, the most common organizational-level response is often reactionary and *ad hoc*. Organizations are not only unaware of how the problem occurred but even of what data they store (Baker et al. 2008), forcing them to learn first and then respond. This apparent absence of formal processes for managing personal information suggests that organizations do not view information as a valuable asset. They would be well-served to treat their information assets with the same care they treat their financial assets.

## Avoid Decoupling

Finally, as the federal and state courts, privacy advocates, and researchers alike have noted, privacy matters are inherently personal (Introna and Pouloudi 1999; Solove 2007b), yet organizations seem unable or unwilling to treat them as such. Often, organizations seem to use complex processes to treat rather personal privacy issues, decoupling actual practice from organizational structures when the expectations of the institutional environment appear to be in conflict with managerial interests (Meyer and Rowan 1977). In doing so, they are more able to shift moral responsibility away from themselves and onto these complex, anonymous organizational procedures and mechanisms (Bunderson 2001). Managers would be wise to base decisions about customer information as if it were their own personal information and not decouple the organizational processes from the personal implications. This new way of thinking would mean managers' asking, when confronting a privacy quandary: How would I feel if *my* information was handled in this way?

In conclusion, because privacy crises such as data breaches are often characterized by indicators that are best observed after the fact, a robust governance program embedded within a culture of moral responsibility should, in our opinion, provide a more effective approach to managing privacy because integrity is integrated into the organization's culture. Even so, no organization can guarantee that it will not suffer a privacy harm in the future. However, the stronger the sense of moral responsibility, as evidenced by the organization's leadership and infused throughout the corporate culture, the more likely the organization will be to have implemented sound technical, structural, and procedural improvements. In doing so, these organizations will have minimized the possibility of such events occurring or the personal impact when these events do occur—thereby upholding their moral duty—while also avoiding costly reputation damage, spillover effects, and legal actions.

## Acknowledgments

We acknowledge the helpful comments of Lynne Markus, Jeff Smith, Alexei Marcoux, and the *MIS Quarterly* reviewers on earlier versions of this paper.

## References

AICPA/CICA. 2006. "Generally Accepted Privacy Principles," Durham, NC: AICPA Information Technology Center (available at http://infotech.aicpa.org/Resources/Privacy/Generally+Accepted+Privacy+Principles/; accessed December 12, 2008).

Aplin, D. G. 2007. "TJX Says at Least 46.2 Million Credit Cards Affected in Computer Hack, FTC Investigating," *BNA Privacy & Security Law Report* (6:14), April 2, pp. 531-532.

Austin, R. D., and Darcy, C. A. R. 2003. "The Myth of Secure Computing," *Harvard Business Review* (81:6), June, pp. 120-126.

Baker, W. H., Hylender, C. D., and Valentine, J. A. 2008. "2008 Data Breach Investigations Report," Basking Ridge, NJ: Verizon BusinessRisk Team (available at http://verizonbusiness.com/resources/security/databreachreport.pdf; accessed June 30, 2008).

Berger, P. L., Berger, B., and Kellner, H. 1973. *The Homeless Mind: Modernization and Consciousness,* New York: Random House.

Bunderson, J. S. 2001. "Normal Injustices and Morality in Complex Organizations," *Journal of Business Ethics* (33), pp. 181-90.

Bureau of National Affairs. 2005. "California Siblings Accessed Information from ChoicePoint in 2000, Documents Show," *BNA Privacy & Security Law Report* (4:10), p. 271.

Bureau of National Affairs. 2007a. "Fraudulent Use of Data Stolen in TJX Breach Reported by Banks; Breach Scope Undefined," *BNA Privacy & Security Law Report* (6:5), January 29, p. 160.

Bureau of National Affairs. 2007b. "TJX Breach Prompts Six States to Consider Merchant Liability; Minnesota Clears Measure," *BNA Privacy & Security Law Report* (6:21), May 21, p. 803.

ChoicePoint. 2008. "Privacy and Information Security Good Practices," LexisNexis ChoicePoint Asset Company (available at www.privacyatchoicepoint.com/common/pdfs/CPPrivacyFactSheet.pdf; April 2008 revision; accessed May 28, 2008).

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., Foxman, E. R., and Ray, A. W. 2008. "Why IT Executives Should Help Employees Secure Their Home Computers," *MIS Quarterly Executive* (7:1), March, pp. 49-55.

Culnan, M. J., and Milberg, S. J. 1998. "The Second Exchange: Managing Customer Information in Marketing Relationships," unpublished working paper, Georgetown University.

Curling, D. C. 2005. "Testimony of ChoicePoint Before the U.S. Senate Committee on the Judiciary, Hearing on Securing Electronic Personal Data: Striking a Balance Between Privacy and Commercial and Governmental Use," April 13 (available at http://judiciary.senate.gov; accessed May 16, 2008).

DeGeorge, R. T. 2006. *The Ethics of Information Technology and Business*, Oxford: Blackwell Publishing Ltd.

DiMaggio, P. J., and Powell, W. W. 1983. "The Iron Cage Revisited: Institutional Isomorphism and Collective Rationality in the Organizational Field," *American Sociological Review* (48:2), pp. 146-160.

Ernst & Young . 2004. "Global Information Security Survey 2004" (available at http://www.ey.com/Global/Assets.nsf/UK/Survey_Global_Information_Security_04/$file/EY_GISS_%202004_EYG.pdf; accessed June 5, 2008).

Federal Trade Commission. 2006. "Press Release: ChoicePoint Settles Data Security Breach Charges; to Pay $10 Million in Civil Penalties, $5 Million for Consumer Redress," January 26 (available at http://www.ftc.gov/opa/2006/01/choicepoint.shtm; accessed June 3, 2008).

Federal Trade Commission. 2008. "Press Release: Agency Announces Settlement of Separate Actions Against Retailer TJX, and Data Brokers Reed Elsevier and Seisint for Failing to Provide Adequate Security for Consumers' Data," March 27 (available at http://www.ftc.gov/opa/2008/03/datasec.shtm; accessed May 21, 2008).

Finkelstein, S., and Hambrick, D. C. 1990. "Top-Management-Team Tenure and Organizational Outcomes: The Moderating Role of Managerial Discretion," *Administrative Science Quarterly* (35:3), pp. 484-503.

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

Goodin, R. 1985. *Protecting the Vulnerable,* Chicago: University of Chicago Press.

Goodpaster, K. E. 1987. "The Principle of Moral Projections: A Response to Professor Ranken," *Journal of Business Ethics* (6:4), pp. 329-332.

Greenaway, K. E., and Chan, Y. E. 2005. "Theoretical Explanations of Firms' Information Privacy Behaviors," *Journal of the Association for Information Systems* (6:6), pp. 171-198.

Introna, L. D., and Pouloudi, A. 1999. "Privacy in the Information Age: Stakeholders, Interests and Values," *Journal of Business Ethics* (22:1), pp. 27-38.

Kerber, R. 2007. "Banks in Region Set to Sue TJX Over Breach," *Boston Globe*, April 25, p. C1.

Lee, R. D., and Mudge, A. R. 2006. "Reasonable Security: The FTC's Focus on Personal Privacy Highlights the Importance of Integrated Information Security Programs," *Privacy & Data Security Law Journal* (7:1), pp. 643-651.

Litan, A. 2006. "Case Study: ChoicePoint Incident Leads to Improved Security, Others Must Follow," ID Number G00142771, Gartner Research, Stamford, CT, September 19.

Luftman, J., and Kempaiah, R. 2008. "Key Issues for IT Executives 2007," *MIS Quarterly Executive* (7:2), pp. 99-112.

Majoras, D. P. 2005. "Prepared Statement of the Federal Trade Commission before the Subcommittee on Commerce, Trade and Consumer Protection, Committee on Energy and Commerce, House of Representatives on Protecting Consumers' Data: Policy Issues Raised by Choicepoint," March 15 (available at http://www.ftc.gov).

Marcoux, A. M. 2003. "A Fiduciary Argument Against Stakeholder Theory," *Business Ethics Quarterly* (13:1), pp. 1-24.

Mason, R. O. 1986. "Four Ethical Issues of the Information Age," *MIS Quarterly* (10:1), pp. 4-12.

Mason, R. O., Mason, F. M., and Culnan, M. J. 1995. *Ethics of Information Management*, Thousand Oaks, CA: Sage Publications.

Meyer, J. W., and Rowan, B. 1977. "Institutionalized Organizations: Formal Structure as Myth and Ceremony," *American Journal of Sociology* (83:2), September, pp. 340-363.

Moore, J. H. 2005. "Why We Need Better Ethics for Emerging Technologies," *Ethics and Information Technology* (7:3), pp. 111-119.

Osterhus, T. L. 1997. "Pro-social Consumer Influence Strategies: When and How Do They Work?," *Journal of Marketing* (61:4), pp. 16-29.

Paine, L. S. 1994. "Managing for Organizational Integrity," *Harvard Business Review* (72: 2), March-April, pp. 79-90.

Pereira, J. 2007. "How Credit-Card Data Went Out the Wireless Door," *Wall Street Journal*, May 4, pp. A1.

Petronio, S. 2002. *Boundaries of Privacy: Dialectics of Disclosure*, Albany, NY: State University of New York Press.

Porter, M. E., and Kramer, M. R. 2006. "Strategy Society: The Link Between Competitive Advantage and Corporate Social Responsibility," *Harvard Business Review* (84:12), December, pp. 78-92.

Power, R. 2008. "CyLab Survey Revals Gap in Board Governance of Cyber Security," CyLab, Carnegie Mellon University, December 2 (available at http://www.cylab.cmu.edu/news_events/cylab_news/governance.html).

Raz, J. 2003. "About Morality and the Nature of Law," *The American Journal of Jurisprudence* (48), pp. 1-15.

Rivlin, G. 2006. "Keeping Your Enemies Close," *New York Times*, November 12 (available at http://www.nytimes.com).

Schwartz, M. 2009. "Europe Debates Mandatory Data Breach Notifications," *The Privacy Advisor* (9:2), p. 1.

Schwartz, P. M., and Solove, D. J. 2008. *Information Privacy: Statutes and Regulations*, Austin, TX: Wolters Kluwer.

Scott, W. R. 2003. *Organizations: Rational, Natural, and Open Systems* (5th ed.), Englewood Cliffs, NJ: Prentice Hall.

Smedinghoff, T. J. 2008. *Information Security Law: The Emerging Standard for Corporate Compliance*, Cambridgeshire, England: IT Governance Publishing.

Smedinghoff, T. J., and Hamady, L. E. 2008. "New State Regulations Signal Significant Expansion of Corporate Data Security Obligations," *BNA Privacy and Security Law Report* (7), October 20, p. 1518.

Smith, H. J. 1993. "Privacy Policies and Practices: Inside the Organizational Maze," *Communications of the ACM* (36:12), pp. 105-122.

Smith, H. J., and Hasnas, J. 1999. "Ethics and Information Systems: The Corporate Domain," *MIS Quarterly* (23:1), pp. 109-127.

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

Solove, D. J. 2007a. "'I've Got Nothing to Hide' and Other Misunderstandings of Privacy," *San Diego Law Review* (44:Fall), pp. 745-772.

Solove, D. J. 2007b. "The New Vulnerability: Data Security and Personal Information," in *Securing Privacy in the Internet Age*, A. Chander, L. Gelman, and M. J. Radin (eds.), Palo Alto, CA: Stanford University Press, pp. 111-136.

Solove, D. J., Rotenberg, M., and Schwartz, P. M. 2006. *Information Privacy Law* (2nd ed.), New York: Aspen Publishers.

Straub, D. W. 1990. "Effective IS Security: An Empirical Study," *Information Systems Research* (1:3), pp. 255-276.

Straub, D. W., Goodman, S., and Baskerville, R. L. 2008. "Framing the Information Security Process in Modern Society," in *Information Security: Policy, Processes and Practices*, D. Straub, S. Goodman, and R. Baskerville (eds.), Armonk: M. E. Sharpe, pp. 5-12.

Straub, D. W., and Welke, R. J. 1998. "Coping with Systems Risk: Security Planning Models for Management Decision Making," *MIS Quarterly* (22:4), pp. 441-469.

Stone, C. D. 1975. *Where the Law Ends*, New York: Harper Torchbooks.

Suchman, M. C. 1995. "Managing Legitimacy: Strategic and Institutional Approaches," *Academy of Management Review* (20:3), pp. 571-610.

U.S. Office of Management and Budget. 2003. *OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002*, Memorandum M-03-22, September 26 (available at http://www.whitehouse.gov/omb/memoranda/m03-22.html; accessed March 1, 2009).

Velasquez, M. 2003. "Debunking Corporate Moral Responsibility," *Business Ethics Quarterly* (13: 4), pp. 531-562.

Velasquez, M. 2006. *Business Ethics: Concepts and Cases* (6th ed.), Upper Saddle River, NJ: Pearson.

Weaver, G. R., Trevino, L. K., and Cochran, P. L. 1999a. "Corporate Ethics Programs as Control Systems: Influences of Executive Commitment and Environmental Factors," *Academy of Management Journal* (42:1), pp. 41-57.

Weaver, G. R, Trevino L. K., and Cochran P. L. 1999b. "Integrated and Decoupled Corporate Social Performance: Management Commitments, External Pressures, and Corporate Ethics," *Academy of Management Journal* (42:5), pp. 539-552.

Weitzner, D. J., Abelson, H., Berners-Lee, T., Feigenbaum, J., Hendler, J., and Sussman, G. J. 2008. "Information Accountability," *Communications of the ACM* (51:6), pp. 82-87.

Williams, C. C. 2008. "ChoicePoint, Inc. and the Personal Data Industry," *Case Research Journal* (27:3/4), Summer/Fall, pp. 115-130.

Xu, H., Dinev, T., Smith, H. J., and Hart, P. 2008. "Examining the Formation of Individual's Privacy Concerns: Toward an Integrative View," in *Proceedings of the 29th International Conference on Information Systems*, Paris (available at http://aisel.aisnet.org/icis2008/6; accessed December 29, 2008).

Yu, T., Sengul, M., and Lester, R. H. 2008. "Misery Loves Company: The Spread of Negative Impacts Resulting from an Organizational Crisis," *Academy of Management Review* (33:2), pp. 452-472.

Zeller, T. 2005. "Breach Points up Flaws in Privacy Laws," *New York Times*, February 24, pp. C1.

## About the Authors

**Mary J. Culnan** is the Slade Professor of Management and Information Technology at Bentley University. She holds a Ph.D. in management from the University of California, Los Angeles. Her current research interests include online communities and information privacy. Her research has been published in *MIS Quarterly, MISQ Executive, Management Science, Organization Science, Journal of Public Policy and Marketing, Information Society*, and *Journal of Interactive Marketing*. She served as a member of the FTC Advisory Committee on Access and Security, and as a Commissioner on the President's Commission on Critical Infrastructure. Currently she serves on the advisory board of the Future of Privacy Forum and as a member of the Government Accountability Office's Executive Committee on Information Management and Technology.

**Cynthia Clark Williams** is the director of the Harold S. Geneen Institute of Corporate Governance at Bentley University and an assistant professor in the McCallum Graduate School of Business. She holds a Ph.D. from the honors program at Boston University and an M.A. from Northwestern University. Her research interests are primarily in the areas of ethics, corporate disclosures, and governance. Her research has been published in *Business Ethics Quarterly*, *Business & Society*, *Case Research Journal, Journal of Business Communication*, and *Public Relations Review.*