June 2009

Data Devolution: Corporate Information Security, Consumers, and Future of Regulation

Andrea M. Matwyshyn

Follow this and additional works at: https://scholarship.kentlaw.iit.edu/cklawreview

Part of the Business Organizations Law Commons, and the Computer Law Commons

Recommended Citation
Available at: https://scholarship.kentlaw.iit.edu/cklawreview/vol84/iss3/2

This Front Matter is brought to you for free and open access by Scholarly Commons @ IIT Chicago-Kent College of Law. It has been accepted for inclusion in Chicago-Kent Law Review by an authorized editor of Scholarly Commons @ IIT Chicago-Kent College of Law. For more information, please contact dginsberg@kentlaw.iit.edu.
DATA DEVOLUTION: CORPORATE INFORMATION SECURITY, CONSUMERS, AND THE FUTURE OF REGULATION

ANDREA M. MATWYSHYN*

INTRODUCTION

Information crime is big business. Identity theft is the fastest growing white-collar crime in the United States, and in 2005, for the third year in a row, it was also the most frequent consumer complaint to the Federal Trade Commission (FTC). According to the FTC, identity theft costs consumers and corporations $50 billion a year. Meanwhile, the exploits of organized information crime are progressively more successful, running armies of remotely controlled computers that allow criminals to attack critical infrastructure targets, such as city power grids.

As these facts indicate, the urgency of addressing the social policy problems arising out of weak information security is clear. The essays in this symposium examine the social policy concerns associated with data vulnerability on three levels of social ecology: governments, markets and

* Andrea M. Matwyshyn is an Assistant Professor of Legal Studies and Business Ethics at the Wharton School of University of Pennsylvania. This symposium arose subsequent to the Data Devolution: Corporate Information Security and the Future of Regulation conference held at the University of Florida Levin College of Law in January 2006. The author wishes to thank the Carol and Lawrence Zicklin Center for Business Ethics Research at the Wharton School at the University of Pennsylvania for research funding support in connection with this symposium.

1. The white-collar crime characterization of identity inadequately reflects the increasing role of organized crime and computer intrusion as integral components in the criminal infrastructure. As such, identity theft is more aptly described as "black-collar crime," combining the financial incentives of white-collar crime with the technological skills of black-hat hackers that organized crime employs.


4. Zombie drones are machines with compromised security that can be controlled remotely without the user's knowledge for malicious purposes, such as to send spam. See, e.g., Primer: Zombie Drone, WASH. POST, Feb. 1, 2004, http://www.washingtonpost.com/wp-dyn/articles/A304-2004Jan31.html; Thomas M. Dailey, Chair and President U.S. Internet Service Providers Ass'n, Gen. Counsel, Verizon Online, Testimony Before the Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census (June 16, 2004).

businesses, and individuals.

I. ANALYZING THE PROBLEM: INFORMATION SECURITY IN SOCIAL CONTEXT

Although a regulatory approach is the likely solution to a portion of the information vulnerability problems we face, government is simultaneously a core part of the vulnerability problem. Governments face a formidable challenge from information crime and the burgeoning criminal black market in stolen data. In particular, data vulnerability on the government level jeopardizes the efficacy of social systems that rely on tight information control. With compromised access controls on government-held data, it becomes impossible to accurately identify individuals using the data in these government databases. Yet, systems such as the social security system continue to rely upon them.

Despite the fact that government databases are attractive targets for information criminals, federal agencies have repeatedly failed cyber security reviews performed by the Government Accountability Office (GAO), and the improvements instituted in response to the GAO warnings of security inadequacy appear to have been largely ineffectual. For example, between 2000 and 2005, the Veteran's Administration (VA) received a failing grade from the GAO cyber security review four out of five times. In 2006, the VA suffered a leakage of 26.5 million veterans' health records. That same year, an offshore subcontractor allegedly tried to extract payment for its services to the agency by threatening to post tens of thousands of veterans' health records that it had access to on the Internet.

Information vulnerability also places businesses at risk, risk not only of criminal prosecutions and civil lawsuits for data breaches, but also potential losses of key corporate assets. Although databases of aggregated consumer information may be the most valuable assets for a business, their value is heavily contingent upon limited access. For example, data breaches at information intermediaries, such as ChoicePoint and Acxiom,

necessarily decrease the value of those databases because value is tied to restricted access. Additionally, weak information security practices may lead to loss of corporate trade secrets and negative publicity.

Further, consumer harm occurs. Information vulnerability, information leakage, and identity theft result in individual consumers' loss of control over their economic identities. Fifteen years ago, the technology revolution shifted power from the center to the periphery.\(^\text{11}\) Now, technology-mediated information aggregation is usurping power back for the center, taking it away from private database owners and consumers, and, sometimes unintentionally, concentrating it in the hands of information criminals. Economic and nonpecuniary harm frequently results from the aggregation and impudent sharing of personal economic histories. A stolen identity, for example, may limit the victim's economic participation in the society for several years.

Unfortunately, without regulatory intervention it is likely that information security will continue to deteriorate on all three levels of social ecology. As more consumers rely on technology-mediated exchange for their daily activities, the incentives for information criminals to engage in information crime rise. An arms race is currently under way between information criminals and technologists, with computer code serving as both a sword and a shield to control information. Progress, if any, is a game of “Whack a Mole” with even major technology companies, such as Microsoft, stating that a regulatory intervention is necessary.\(^\text{12}\) Borrowing the words of Lewis Carroll, our society is experiencing an information security “Red Queen Effect,” a situation similar to one where Alice tells the Red Queen that she needs to run simply to stay in the same place and needs to run twice as fast to advance.\(^\text{13}\) Thus, as the arms race continues between information criminals and information security professionals, consumers, like Alice, are forced to adjust quickly to the escalating information crime threats simply in order to survive.

II. The Legislative Landscape

The legal information security regime in the United States is a patchwork of federal and state laws. The federal regulatory approach is segmented by the type of collected and stored data. For example, the

\(^{11}\) See, e.g., Andrew L. Shapiro, The Control Revolution xiii (1999).


\(^{13}\) See Lewis Carroll, Through the Looking Glass and What Alice Found There (1872).
Health Insurance Portability and Accountability Act regulates health data, while the Gramm-Leach-Bliley Act regulates financial data, and the Children's Online Privacy Protection Act regulates children's data. Most states have also recently passed data breach notification laws that require entities to report data leaks to impacted consumers.

Although federal and local state statutes have been in place for several years, they have had limited success. Their efficacy remains in doubt as the problem of identity theft escalates, and the number of data breaches increases. Therefore, a thoughtful reevaluation of the United States domestic regulatory direction in the area of consumer protection is warranted.

A. Information Security Obligations under Federal Law

1. Information Security Obligations under the Health Insurance Portability and Accountability Act

In the area of health data privacy, the Health Insurance Portability and Accountability Act of 1996 (HIPAA) sets minimum levels of data care and security with regard to collection, storage, and sharing of personally identifiable health information. Specifically, HIPAA requires that entities that handle personally identifiable health information give notice of their privacy practices and ensure privacy and security of information. HIPAA includes privacy rules and security rules. HIPAA privacy rules require that responsibility for privacy within each organization be centralized in the hands of a Chief Privacy Officer. Security rules mandate that entities covered by HIPAA implement administrative, physical, and technical safeguards against data breaches. Finally, both privacy and security rules mandate disclosure of privacy and security practices to consumers.

16. Id. §§ 164.302-.534.
17. Entities must designate a privacy official who is responsible for developing and implementing the entities' privacy policies and procedures and a contact person or officer who is responsible for receiving complaints. Id. § 164.530(a). Many companies that do not handle health information have also begun to designate officer level privacy positions. PRICEWATERHOUSECOOPERS LLP, KEY REGIONAL HIGHLIGHTS FROM THE INFORMATION SECURITY SURVEY 1 (2008).
19. 45 C.F.R. §§ 164.502(e), .504(e).
and require that each contract with a third party provider includes an information security warranty on the part of the provider to maintain integrity, confidentiality, and availability of health data that the provider receives.

But the enforcement of HIPAA rules has been weak in the past. During a conference on HIPAA privacy rules, Richard M. Campanelli, then Director of the U.S. Department of Health and Human Services (HHS) Office of Civil Rights stated that HHS would not be aggressive in punishing healthcare organizations that violate HIPAA. Campanelli indicated that voluntary compliance was the most effective way to implement data security, and voluntary compliance would be achieved by the public complaining directly to healthcare organizations about any privacy breaches. This spirit of non-enforcement appears to continue with few actions brought to date.

2. Information Security Obligations under the Gramm-Leach-Bliley Act

The Financial Modernization Act of 1999, also known as the Gramm-Leach-Bliley Act (GLB Act), governs the handling of data by financial institutions. The GLB Act requires that financial institutions provide notice of their privacy practices, exercise care in handling data, and allow

20. Id. pts. 160, 162, 164.


Additionally, foreign companies to which domestic organizations have outsourced work with patient data have threatened to publish the patient records on the Internet unless the domestic entity paid a “ransom” to prevent such disclosure. See Dr. Richard Bassett et. al., Security Risks Associated with Geosourcing, INFO. SYS. SEC. ASS’N J., Sept. 2004, at 22–28. But the first criminal prosecution under HIPAA was settled in August 2004 in an egregious case of patient information theft by an insider who used patient data to obtain credit cards. Plea Agreement, U.S. v. Gibson, No. 04-0374, 2004 WL 2237585 (W.D. Wash. Aug. 19, 2004).


consumers to opt out of data sharing and to prohibit use of their private financial information in ways they did not authorize. The GLB Act also requires that contracts between financial institutions and partners with whom they share data prohibit the partners’ use of customer information for any purpose other than the initial information disclosure.

More than ten federal and state agencies are authorized to enforce various provisions of the GLB Act, and several entities have been prosecuted for violations of the statute. Further, not only does the GLB Act define "financial institutions" broadly, but the FTC has also attempted to expand the reach of the GLB Act to businesses that are not generally considered “financial institutions” under the FTC.  

3. Information Security Obligations Under the Children’s Online Privacy Protection Act

The Children’s Online Privacy Protection Act (COPPA), which was enacted in October 1998, requires that websites targeting children under the age of thirteen provide notice of their privacy practices and obtain verifiable parental consent before collecting data from children. The

25. 16 C.F.R. § 313.13.
26. The FTC prosecuted Superior Mortgage Corporation (“Superior Mortgage”), a lender with forty branch offices in ten states operating multiple websites, for violating the GLB Act. Compl. ¶ 1, In re Superior Mortgage Corp., No. C-4153 (Fed. Trade Comm’n Dec. 16, 2005). The FTC alleged that the company, among other things, “failed to implement reasonable policies and procedures to protect the security and confidentiality of the information it collect[ed].” Id. ¶ 5. More specifically, it alleged that Superior Mortgage violated the GLB Act Safeguards Rule by failing to:

[(i)] assess risks to its customer information [in a timely manner]; [(2)] institute appropriate password policies to control access to company systems and documents containing sensitive customer information; [(3)] . . . encrypt or otherwise protect sensitive customer information [before emailing it]; and (4) . . . ensure that its service providers were providing appropriate security.

Id. ¶ 6. The FTC’s encryption argument is noteworthy; it asserts that although the company encrypted sensitive personal information when it was collected, it was decrypted and e-mailed in clear, readable text once the information was received at the website. Id. The FTC concluded that it had reason to believe that Superior Mortgage had violated the GLB Act and ordered Superior Mortgage to (1) establish data security procedures subject to independent third-party auditor review for ten years; and (2) not misrepresent the extent to which the company maintains and protects privacy, confidentiality, or security of consumer personal information. See In re Superior Mortgage Corp., No. C-4153 (Fed. Trade Comm’n Dec. 14, 2005).


28. Id. §§ 6501–6502. For a discussion of COPPA, see, for example, Gaia Bernstein, When New Technologies Are Still New: Windows of Opportunity for Privacy Protection, 51 VILL. L. REV. 921, 927, n.19 (2005); Andrea M. Matwyshyn, Material Vulnerabilities: Data Privacy, Corporate Information Security, and Securities Regulation, 3 BERKELEY BUS. L.J. 129, 133 (2005). Commentators have observed that COPPA was a reaction to the failure of self-regulation, particularly subsequent to
DATA DEVOLUTION

The statute also empowers the FTC to promulgate additional regulations to require website operators subject to COPPA to establish and "maintain reasonable procedures to protect the confidentiality, security, and integrity of personal information collected from children." According to the FTC, appropriate security measures for protecting children's data include "using secure web servers and firewalls; deleting personal information once it is no longer being used; limiting employee access to data and providing those employees with data-handling training; and carefully screening the third parties to whom such information is disclosed."

But, COPPA leaves some data security to the discretion of individual website operators and creates no external reporting mechanism to monitor their internal security improvements. Specifically, as mentioned above, COPPA stipulates that a website "operator" must obtain "verifiable parental consent" before collecting data from children under thirteen. The guidance offered on operationalization is limited. Although a fax from a parent is the preferred method of parental consent verification per the statute, email verification was permitted due to the cumbersome nature of fax verifications. However, the actual verifiability of these methods warrants scrutiny.

The FTC applies a "sliding scale" approach to COPPA inquiries. The FTC's analysis varies depending on the character of data collection and intended use of the collected data because the need to obtain verifiable parental consent does not apply equally to all child data gathering. For example, for the FTC, a situation where a website collects data for a one-time use without permanently connecting the child with the information


30. Children's Online Privacy Protection Rule, 64 Fed. Reg. 59,888, 59,906 (Nov. 3, 1999) (to be codified as 16 C.F.R. pt. 312). But these technology specifications are suboptimal. For example, servers cannot be inherently "secure" or "vulnerable"; securing a server is an ongoing process. A better regulation would require companies to take all steps that a leading security research firm has identified as fundamental to the exercise of care in attempting to secure a server on an ongoing basis.
31. Id. Encryption was deemed to be potentially cost prohibitive and left to the discretion of entities, as was the suggested use of contractual provisions that required that third parties follow minimum standards of data handling if they had been granted access to the collected children's data. Id.
32. 15 U.S.C. § 6501(2) (defining "operator" broadly to encompass everyone who meaningfully handles children's data); Id. § 6502.
33. Children's Online Privacy Protection Rule, 16 C.F.R. § 312.5 (2005). Email verification was original intended as a temporary measure, but its use has persisted over time. Still, email verification is susceptible to even easier child circumcision than fax verification.
34. See BNA, FTC Decides to Retain COPPA Rule With No Change After Review of Comments, 7 COMP. TECH. L. REP. 127 (2006).
does not legally require the same degree of consent verifiability as a situation where a website establishes such permanent connection between the child and the information.\footnote{See 15 U.S.C. § 6503(2). In particular, one of the COPPA exceptions provides for one time collection, provided the information is subsequently destroyed. Id. § 6503(2)(A). In practice, companies frequently use these exceptions to the extent possible to avoid compliance. Id.} Additionally, the FTC has permitted the Children’s Advertising Review Unit of the Better Business Bureau to serve as a safe harbor program to review and warrant websites’ compliance with COPPA.\footnote{36. See Consent Decree & Order for Civil Penalties, Injunction, and Other Relief, U.S. v. Xanga.com, Inc., No. 06-CIV-6853(SHS) (S.D.N.Y. Sept. 7, 2006).}

The FTC has authority to institute regulatory prosecutions against entities violating COPPA. These prosecutions result in fines and consent decrees. The fines range from $130,000 against Industrious Kid, Inc.\footnote{37. See Consent Decree & Order for Civil Penalties, Injunction, and Other Relief, U.S. v. Industrious Kid, Inc., No. 3:08-cv-00639 (N.D. Cal. Jan. 6, 2008).} to, as of recently, $1,000,000 against Xanga.com, Inc.\footnote{38. See Consent Decree & Order for Civil Penalties, Injunction, and Other Relief, U.S. v. Xanga.com, Inc., No. 06-CIV-6853(SHS) (S.D.N.Y. Sept. 25, 2006).} Generally, however, they do not exceed $500,000.\footnote{39. See Consent Decree & Order for Civil Penalties, Injunction, and Other Relief, U.S. v. Industrious Kid, Inc., No. 3:08-cv-00639 (N.D. Cal. Jan. 6, 2008).} Further, as of 2009, only fifteen entities appear to have been prosecuted according to the FTC since the enactment of COPPA.\footnote{40. See Consent Decree & Order for Civil Penalties, Injunction, and Other Relief, U.S. v. Hershey Foods Corp., No. 4:03-CV-00350 (M.D. Pa. Feb. 26, 2003).}

For these and other reasons, COPPA has received mixed reviews. The deterrent effect of prosecutions appears to be limited. A large number of websites subject to COPPA are noncompliant and willing to risk prosecution instead of attempting to comply with COPPA: several studies indicate that less than only 70% of the reviewed websites attempt to comply with COPPA.\footnote{41. See, e.g., JOSEPH TUROW, PRIVACY POLICIES ON CHILDREN’S WEBSITES: Do THEY PLAY BY THE RULES? 12 (2001). Two studies of COPPA compliance by the University of Pennsylvania’s Annenberg Public Policy Center and by the Center for Media Education revealed that although most of the reviewed websites had privacy policies, those privacy statements did not include the required disclosures and used language that was difficult to understand. Id.} Businesses have complained that the estimated
annual cost of COPPA compliance through monitoring use of the website, drafting privacy policies, and obtaining proof of parental consent is as much as $200,000. In some cases, companies have deemed the costs of compliance prohibitive and simply ceased all or parts of their operations. For example, some websites removed interactive elements from their sites shortly after the enactment of COPPA, alleging that compliance costs rendered those lines of business unsustainable.

But the biggest problem is, practically speaking, that COPPA protects only the data of children who wish to have it protected. For example, a COPPA-compliant website may require a child to enter a birth date, and, if the child is under thirteen, initially deny such child access to the content. But this age verification process is easy to circumvent: a child wishing to access content after having been denied access may log into the website again and provide a false birth date to gain access to the material.

B. Information Security Obligations under State Data Breach Notification Laws

State data breach notification statutes are the newest and, arguably, most effective approach to addressing data security issues. At least forty-eight states have data security breach notification statutes that compel entities that have suffered data breaches to provide written notice to the consumers whose data has been impacted. The legislative purpose of data breach notification laws was to prevent identity theft and to generate a modicum of external accountability for data care: legislators have aimed to mitigate the effects of identity theft by requiring entities to notify consumers of data compromised during a data breach. Alerting potential victims to check their credit reports may help detect some instances of identity theft early. Meanwhile, research indicates that consumers who

44. Id.
46. Id.
47. Id.
48. For a discussion of state data breach notification statutes see, for example, Paul M. Schwartz, Notification of Data Security Breaches, 105 MICH. L. REV. 913, 915 (2007).
take notice of data breach notifications increasingly view information holders as having an obligation of data stewardship to them. \textsuperscript{51} But consumers may also feel powerless to protect themselves against the mishandling of their data and, therefore, develop "notification fatigue" as they receive numerous security notices describing past breaches. \textsuperscript{52}

There are significant differences among state data breach notification laws. For example, state statutes vary in the types of data that they cover: in California, breach of medical data triggers the statutory disclosure obligation, \textsuperscript{53} while other states exempt encrypted data from the types of information that trigger the notice requirement, with the definition of encrypted data further varying among states. The states also define "breach" differently, oftentimes allowing an entity that has suffered a data-compromising incident to determine whether it has to give notice to the consumers. There are also significant variations in the statutory timeframes for reports of security breaches, with some statutes allowing as much as ten days or longer to report a breach after the company discovers it. \textsuperscript{54} But the discovery of a breach may occur months or years after the initial communication with an individual. \textsuperscript{55} Finally, the party that must give notice varies, depending on the state statute. Most, but not all, of the statutes cover only for-profit entities, and prosecutions have been limited. \textsuperscript{56}

\textbf{C. Information Security Obligations under Securities Law and the Sarbanes-Oxley Act}

Securities law provides another source of information security

\footnotesize{id theft/ con_steps.htm (last visited Dec. 15, 2009).}


\textsuperscript{52} See, e.g., Grant Gross \textit{Analysis: US Data Breach Notification Law Unlikely This Year}, MACWORLD, May 8, 2006, \url{http://www.macworld.com/article/50709/2006/05/databreach.html} (discussing the possibility of national data breach notification legislation).

\textsuperscript{53} Deborah Gage, \textit{Notification Law to Now Cover Medical Data; State Residents Must be Told If Records Breached}, S.F. CHRON., Jan. 4, 2008, \url{http://www.sfgate.com/cgi-bin/article.cgi?f=/c/a/2008/01/04/BUR6U900O.DTL}.

\textsuperscript{54} N.J. STAT. ANN. § 56:8-163 (West 2008).

\textsuperscript{55} The University of California, Los Angeles, suffered breaches of data of applicants from the previous ten years. See, e.g., Gregg Keizer, \textit{UCLA Admits Massive Data Hack}, INFORMATIONWEEK, Dec. 12, 2006, \url{http://www.informationweek.com/security/showArticle.jhtml?articleID=196603485}.

\textsuperscript{56} One of the prosecutions involved a claims management company, CS Stars LLC ("CS Stars"). SANS Institute, \textit{NY AG Settles Data Breach Case with Chicago Company}, SANS NEWSBITES, Apr. 27, 2007, \url{http://www.sans.org/index.php?display.aspx?id=3474}. The New York Attorney General’s alleged that CS Stars violated New York’s Information Security Breach and Notification law because it waited two months after discovering that a computer containing personnel records was missing to notify 540,000 individuals about the breach. \textit{Id.} The AG reached a settlement agreement with the company, which had to pay $60,000 for the AG investigation costs. \textit{Id.}
obligations for publicly traded companies. Business norms disclosed in securities filings shape, in part, the standards of reasonable behavior in the area of information security.

Securities and Exchange Commission (SEC) regulations may already (and should explicitly) require discussions of security practices and data breaches as part of securities filings. For example, Item 103 of Regulation S-K ("Item 103"), requires entities to disclose "material pending legal proceedings other than ordinary routine litigation incidental to the business." Prudent companies should disclose pending information security litigation, particularly involving possible information security harms. Such litigation frequently involves class action suits, which may result in large damage awards against the company and generate bad publicity; companies should not deem such lawsuits to be "ordinary routine litigation" exempt from disclosure.

Item 308 of Regulation S-K ("Item 308") requires management to report on internal controls over financial reporting. More specifically, Item 308(a)(2) requires a statement identifying the framework that management uses to evaluate the effectiveness of the company's internal controls. The SEC should ensure that companies disclose information security audits, such as SAS 70 audits, as part of this statement. Under Item 308, a company must also provide an attestation report of a registered public accounting firm on the internal controls over financial reporting. Further, Item 308(a)(3) requires management to disclose material weaknesses in internal controls over financial reporting, which may include serious information security breaches. If an entity experiences repeated data vulnerabilities, particularly serious intrusions by third parties into information systems, it is possible that the integrity of the entity's financial auditing processes has been corrupted. Under such circumstances, attestation of integrity may be improper. Similarly, both the SEC and an entity must consider the extent of the diminished value of compromised data and its impact on the value of intangible assets reported in the financial statements.

58. Id. § 229.308.
59. Id. § 229.308(a)(2).
60. SAS 70 audits pertain to an in-depth audit of a service organization's control activities, which generally include an inspection of controls over information technology and other security processes. See SAS 70 Overview, http://www.sas70.com/about.htm (last visited Dec. 1, 2009).
61. 17 C.F.R § 229.308(a)(2).
62. Id. § 229.308(b).
63. Id. § 229.308(a)(3).
64. Id. § 229.308(b).
Form 10-K, an annual report, requires that public entities disclose all "material" events related to the business that may impact a shareholder's investment in the entity.\(^5\) The goal of the Management Discussion and Analysis of Financial Condition and Results of Operations ("MD&A")—one of the central requirements of the annual report—is to enable investors to analyze the management's view of the corporation's financial health, culture, goals, and identity.\(^6\) Therefore, this section is intended to require a discussion of trends, unusual or important events, and corporate risks that are reasonably likely to materially impact the company through the eyes of management.\(^6\) Although the definition of materiality is in flux and grants the corporation discretion in identifying "material" events,\(^6\) the SEC should consider the risks of information security breaches. Particularly those breaches that involve data-intensive enterprises should be deemed material, and, therefore, subject to the disclosure requirements.\(^6\) Therefore,


66. Id. § 229.303; Release No. 33-6835 (May 18, 1989) ("The MD&A requirements are intended to provide, in one section of a filing, material historical and prospective textual disclosure enabling investors and other users to assess the financial condition and results of operations of the registrant, with particular emphasis on the registrant's prospects for the future."). The MD&A "shall provide information as specified in paragraphs (a)(1) through (5) of this Item and also shall provide such other information that the registrant believes to be necessary to an understanding of its financial condition, changes in financial condition and results of operations." 17 C.F.R. § 229.303; see also Commission Guidance Regarding Management's Discussion & Analysis of Financial Condition and Results of Operations, SEC Release No. 33-8350 (Dec. 29, 2003) (emphasizing that MD&A requires both analysis and discussion, and should not simply be a restatement of the financial statement in narrative form nor an otherwise uninformative series of technical responses to MD&A requirements). Further:

The Commission has long recognized the need for a narrative explanation of the financial statements, because a numerical presentation and brief accompanying footnotes alone may be insufficient for an investor to judge the quality of earnings and the likelihood that past performance is indicative of future performance. MD&A is intended to give the investor an opportunity to look at the company through the eyes of management by providing both a short and long-term analysis of the business of the company. The Item asks management to discuss the dynamics of the business and to analyze the financials.

67. Item 303(a)(3) requires disclosure of "known trends or uncertainties that have had or that the registrant reasonably expects will have a material favorable or unfavorable impact" on future income. 17 C.F.R. § 229.303(a)(3)(ii).


69. Courts have defined materiality differently in different contexts of securities law. In some instances, courts apply a "probability-magnitude" test. See, e.g., Basic Inc. v. Levinson, 485 U.S. 224, 239 (1988). Under this test, materiality depends on whether the magnitude of the potential loss is so great that even a remote risk requires disclosure or provides basis for actions for fraud under Section 10b-5. See, e.g., Secs. & Exch. Comm'n v. Tex. Gulf Sulphur, 401 F.2d 833, 849, 867 (2nd Cir. 1968). In 1988, the SEC adopted this standard of materiality for MD&A disclosures. See Fed. Sec. Law Rep. Rel. No. 25951, 62,125, 62,126 (1988). But in 1989, the SEC explained that the MD&A materiality standards differed from those adopted in *Texas Gulf Sulphur*, 401 F.2d at 849. The SEC instructed management to make two assessments to determine materiality: (1) assess whether a particular trend,
good corporate practice should include discussions of information security strategy, diligence in monitoring, policies, and enforcement habits in the annual report. The MD&A disclosures also complement “risk factor” disclosure in registration statements under the 1933 Securities Act and increasingly form an integral part of periodic reporting under the 1934 Exchange Act. Additionally, the MD&A disclosures create a public record of diligence in addressing information security that may prove useful in litigation after a security breach.

The Public Company Accounting Reform and Investor Protection Act of 2002, commonly known as the Sarbanes-Oxley (“SOX”), and the new rules promulgated under SOX enlarged the scope of the discussion required in MD&A. Section 404 of SOX (“Section 404”) addresses the accuracy of audit processes and the security of corporate information of publicly event, or uncertainty is reasonably likely to happen; and (2) if management cannot determine the likelihood of such occurrence, it must evaluate the contingency on the assumption that it will happen. Management's Discussion & Analysis of Financial Condition & Results of Operations; Certain Investment Company Disclosure, SEC Release No. 33-6835 (May 18, 1989). A different definition of materiality appears in insider trading contexts. Information is material for purposes of creating the basis of an insider trading action if “there is a substantial likelihood that a reasonable shareholder would consider it important” in deciding how to act. See TSC Indus., Inc. v. Northway, Inc., 426 U.S. 438, 449 (1976).


traded entities. It requires that entities establish adequate internal controls and auditing procedures certified by management regarding the financial statements of the entity. Consequently, SOX addresses information security in two ways. First, entities must establish information security processes and audit procedures to protect against information vulnerability. Second, entities must accurately reflect the diminished value of any intangible assets compromised by information security breaches on their financial statements. In other words, information regarding the value of intangible assets, which includes both consumer information and corporate trade secret information, must be accurately reported. Similar to the requirement under Item 308 of Regulation S-K, if the data has been compromised, the reported value must reflect this negative change in value.

D. Information Security Obligations under the Federal Trade Commission Act and state law

Section 5 of the FTC Act gives the FTC authority to examine entities' "unfair or deceptive" information practices. The FTC has interpreted Section 5 of the FTC Act to mean that a representation, omission, or practice is "deceptive" if it is likely to (1) mislead consumers and (2) impact consumers' decisions about a particular product or service. According to the FTC, an act or practice is "unfair" under the FTC Act if an injury that results or is likely to result is (1) substantial, (2) not outweighed by other benefits; and (3) not reasonably avoidable. The FTC has already relied on these definitions to bring action against companies that have experienced data breaches, particularly when no other data

73. For example, one auditing procedure that specifically relates to information security is a SAS 70 audit. See SAS 70 Overview, http://www.sas70.com/about.htm (last visited Nov. 11, 2009).
74. Section 302 of SOX requires the SEC to promulgate rules regarding officers' responsibility to certify the accuracy of financial statements and auditing procedures. See Final Rule, Certification of Disclosure in Companies' Quarterly and Annual Reports, Certification of Disclosure in Companies' Quarterly & Annual Reports, SEC Release Nos. 33-8124 (Aug. 29, 2002).
76. Because Section 302 of SOX specifically authorizes the SEC to promulgate rules regarding officers' responsibility to certify the accuracy of financial statements and auditing process, the SEC is authorized to promulgate rules specific to information security reporting and certification in connection with Section 404 of SOX. Public Company Accounting Reform and Corporate Responsibility Act, 15 U.S.C. § 7241.
77. Id. § 45.
78. See id. § 6502 (making it unlawful for a website to misrepresent why it is collecting children's personal identifying information without clearly and prominently disclosing the additional data use).
security statute governs the leakage of data. Thus, a business's data security practices may trigger scrutiny not only under specific data privacy statutes, but also under the general FTC Act.

In addition to the FTC Act, many states have consumer fraud laws, known as the "Little FTC Acts," that often authorize private citizens to recover damages and attorney fees for loss resulting from the merchant's deceptive practice. The remedies under state and local consumer fraud laws are often stronger than those under similar federal statutes; they also apply to more seller practices than do federal laws.


[(1)] created unnecessary risks to sensitive information by storing it in multiple files when it no longer had a business need to keep the information; [(2)] failed to use readily available security measures to limit access to its computer networks through wireless access points on the networks; [(3)] stored the information in unencrypted files that could be easily accessed using a commonly known user ID and password; [(4)] failed to limit sufficiently the ability of computers on one in-store network to connect to computers on other in-store and corporate networks; and [(5)] failed to employ sufficient measures to detect unauthorized access.

Id.

81. Marketing is the most data intensive portion of business operations where issues of deceptive or unfair practices arise. Consequently, data security risks related to consumer data may be at their greatest in connection with marketing uses. In addition to the FTC Act concerns, businesses may face liability under the Controlling the Assault of Non-Solicited Pornography and Marketing Act ("CAN-SPAM Act"), which became effective on January 1, 2004. 15 U.S.C. §§ 7701–7713 (2006). The CAN-SPAM Act makes it unlawful to send messages with materially false or misleading header information, which includes the subject, and prohibits address harvesting and dictionary attacks. Id. § 7704(a). It also requires that spam email provide an option to opt out of future mailings, that such opt-out requests be honored, and that sexually explicit materials be clearly labeled as such. Id. § 7704(a)(5), (d). Businesses that are not sufficiently careful in complying with individual consumer requests and controlling their data may face suit from the FTC, state regulators, or ISPs on behalf of consumers. Id. § 7706. Although the CAN-SPAM Act creates private right of action for the Internet Service Providers (ISPs), it preempts most state anti-spam statutes. Id. As such, it takes away the private right of action that non-IPS businesses and consumers had against spammers under state anti-spam statutes against spammers.

82. For a discussion of the little FTC Acts, see, for example, MARY DEE PRIDGEN, CONSUMER PROTECTION AND THE LAW (2008 ed.). Outside of the little FTC Acts governing data security related to marketing practices, state statutes, which included provisions addressing matters not specifically contemplated by the Act, may provide recourse for parties impacted by spam, although the CAN-SPAM Act preempted a majority of state spam statutes. Therefore, recourse and potential liability for sending unsolicited commercial email pertains on the state level only in selected states. As of December 2003, immediately before the CAN-SPAM Act went into effect, thirty-one states had laws regulating the transmission of spam. None of these statutes contained an outright ban on spam, but they (1) restricted either the categories of recipients of spam to those with a preexisting relationship with the sender or to those who otherwise affirmatively consented to spam email; or (2) required clear labeling through a subject line containing the letters ADV or an opt-out method in the text of the spam to prevent the future sending of spam to this recipient. Until recently, neither the state attorney generals, nor private spam recipients brought action under these statutes. See e.g., Gillman v. Sprint Commc'ns, 91 P.3d 858, 859 (Utah Ct. App. 2004); Verizon Online Servs, Inc. v. Ralsky, 203 F. Supp. 2d 601, 602, 604, (E.D. Va. 2002); MonsterHut Inc. v. PacTeC Commc'ns, Inc., 294 A.D.2d 945, 946 (N.Y. App. Div. 2001); State of Wash. v. Heckel, 24 P.3d 404, 405 (Wash. 2001); Compl. ¶¶ 5–14, Microsoft Corporation v. Does 1 through 50, No. 5:03-cv-00644 (N.D. Cal. Feb. 14, 2003); Compl. ¶¶1–4, Morrison & Foerster v. Etracks.com, Inc, No. 404294 (CA. Supr. Ct. June 12, 2002). Courts have upheld the constitutionality of
Further, generally, under the basic principles of states' corporate law, officers and directors of a corporation owe the shareholders three fiduciary duties: the duty of care, loyalty and good faith. Arguably, corporate disregard for data security raises an issue of breach of duties of care and good faith, which, broadly speaking, require that directors and officers act in good faith with the care of a prudent person in their decision making process and in the best interest of the corporation. The issue becomes whether the fiduciaries' data protection actions are in line with the exercise of reasonable care in decision making that a prudent person would exercise regarding the manner in which corporate information assets are acquired, used and protected.

Particularly in data-intensive and intellectual property-intensive enterprises, much corporate capital is allocated to research and development of new intellectual property. This new intellectual property can arise in three forms: traditional research and development projects whose output will be protected through copyright, trademark or patent law; top secret innovation protected solely by trade secret law and contracts; and databases of consumer information, potentially protectable through either method. Particularly for the corporate intangible assets that are best protected through trade secret law, this legal protection depends on the maintenance of confidentiality of the asset. Courts look to whether entities have taken reasonable steps to preserve the secrecy of the asset to determine whether trade secret protection should be extended. If an entity has a history of security breaches, it is difficult to argue that an entity has engaged in careful, systematic protection of its information assets. Consequently, each security breach may jeopardize trade secret protection for key corporate assets and, correspondingly, signal a possible inadequate level of care on the part of corporate decision makers.

Because of statutory prescriptions regarding proper data handling in connection with certain types of data, security breaches of consumer information databases may result not only in prosecution by the FTC, the state attorney general, and other agencies, but also in consumer class actions and severe losses of goodwill. Research demonstrates that in at least some instances 19% of customers terminate their relationship with the company after a data security breach, 40% consider terminating the relationship, and approximately 5% hire attorneys for potential legal


These numbers are significant particularly when one considers that between twenty-three and fifty million people have received notices of data breaches in 2005.\textsuperscript{85} Because of the severity of potential negative consequences an entity may suffer from a security breach, officers and directors who choose to ignore correction of information security problems within the entity may be deemed to breach their fiduciary duties. Their failure to protect corporate assets may rise to the level of corporate conduct not protected by the business judgment rule.

\textit{E. Contractual Information Security Obligations}

In addition to the statutory obligations discussed above, contract law is the primary source of data security obligations. Contractual obligations, as memorialized in connection with particular data exchanges, become a source of both potential leverage and liability.

The statutes noted previously require data security representations and warranties for transfers of certain types of data between business partners, such as for the transfers of financial data under the GLB Act.\textsuperscript{86} But, even in data sharing situations not covered by statutes, prudent counsel should draft contract provisions specifically addressing the standards of sharing, storing, using, transferring and deleting data, handling security audits and data security breaches, and allocating expenses associated with data breaches. The contract should also provide a roadmap for delineation of data security responsibilities. These types of provisions offer a method of risk management, forming a written record that may be useful when assigning responsibility after a data breach.

With respect to consumers, privacy policies are the most prevalent data security contracts. The FTC enforces these policies as contracts by bringing action for unfair or deceptive practices for their breaches.\textsuperscript{87} Similarly to the FTC, courts tend to analyze privacy policies as contracts, with data security obligations surviving even in bankruptcy.\textsuperscript{88}

\begin{flushleft}
\textsuperscript{84} Id.
\textsuperscript{85} Id.
\end{flushleft}
F. Common Law Information Security Obligations

Information security common law, particularly involving claims of negligent handling of data, has begun to emerge; as a practical matter data security statutes cover relatively few categories of data and leave many data care obligations to the discretion of corporate actors. Claims of data security negligence in various contexts have survived summary judgment, and the frequency of such claims has continued to increase. The development of the common law of information security negligence claims may eventually result in clear legal construction of “reasonable” security practices, “reasonable” corporate conduct in contracting, and “reasonable” users. However, additional regulatory approaches will also be needed.

One of the recent cases involving allegations of information security negligence arose out of a security breach of TJX Companies, Inc. (“TJX”). In 2005, computer hackers obtained at least 45.7 million credit and debit card numbers from TJX’s database. At the time of the breach, TJX’s wireless network was protected with WEP, an obsolete form of encryption that was less secure than the encryption mechanism used on many home wireless networks. TJX’s estimated direct monetary losses from the incident were between $1.35 billion and $4.5 billion.

Numerous lawsuits alleging negligence in information security and


90. Just as with any negligence claim, a plaintiff in an information security negligence claim must show that (1) a duty existed on the part of the defendant to keep data secure in accordance with a specific standard of conduct in order to protect the plaintiff against an unreasonable risk of injury; (2) the defendant breached this duty of data security; (3) this breach was the cause of the plaintiff’s injury; and (4) the plaintiff suffered quantifiable damages because of the data security breach.


data handling were filed following the breach. Although most of these types of claims will likely settle, claims by banks and other larger entities that incur losses as a result of breaches will likely continue to be litigated. Therefore, in the TJX case, in addition to TJX's direct losses from the data breach, the company would also incur the costs of settlement payouts and, potentially, damage awards from remaining litigation. According to TJX's estimates, it would cost the company more than $150 million to correct its security problems and settle with consumers that were impacted by the breach.

III. THE EMBEDDEDNESS OF INFORMATION AND VULNERABILITY

The difficulty in addressing the problems of information vulnerability arises, in part, from the fact that data vulnerability is driven by social context and emergent structures. Dynamic interactions of multiple actors have resulted in aggregate behaviors and norms that have shaped the nature of the current data security policy dilemma. Blending the insights from many disciplines, our policies must be flexible enough to absorb the emerging strategic behavioral responses of corporations, criminals, and consumers. First and foremost, our analytical models must be reframed around an interdisciplinary policy-driven and problem-driven inquiry, rather than a strictly legal or technological one.

Thus, the broader goal of this symposium is to advance the generation of an international and interdisciplinary discourse on issues relating to information security. The contributors on this issue span multiple disciplines and countries. Each author approaches the policy problem of information vulnerability from a different perspective, yet all of them agree on the need of an interdisciplinary analysis.

The pieces are organized in three thematic sections. The first section presents a conceptual introductory framework, followed by a practical survey of the current state of information security problems in the United States. The second section introduces the inherent duality of digital data as,
simultaneously, property of the corporations and living persons; the section then discusses corporate information security as a means of protecting both intellectual property and personal data of individual citizens. The third section discusses information security obligations under current United States law and under possible future regulations.

A. Introduction to Information Security as a Policy Issue

Philip Howard and Kris Erickson introduce the practical challenges of addressing information security as a policy matter. Philip Howard, a professor of cyber culture studies in the Department of Communication at the University of Washington, in joint work with Kris Erickson from the Department of Geography at the University of Washington, sets forth the empirical reality about the prevalence of information security breaches and data leakage in both the corporate and the public sectors. Data breaches between 1995 and 2006 demonstrate the vulnerability trends. During this time, government agencies, firms, hospitals, universities, and the military reported approximately 1.9 billion records as compromised due to the information criminals hacking into systems and organizations mismanaging information security. The escalating frequency and severity of breaches presents an empirical case for addressing information security issues head-on as a policy matter. Computer hacking has been widely blamed as the primary cause of information vulnerability, obfuscating other contributing causes of the problem. Similarly, Howard and Erickson argue that the responsibility of commercial, educational, government, medical, and military organizations for data security breaches has been erroneously downplayed. The scale and scope of information loss over the past decade would suggest that organizational self-regulation or self-monitoring is failing.

B. Information Security and the Dual Nature of Consumer Data Held by Corporations

Section two introduces key questions of intellectual property that impact information security. An inherent duality exists in personally identifiable information collected by corporations and governments. The collector acquires an interest in the collected data, which becomes the collector's intangible asset, while the consumers retain residual dignitary or property interest in the same data. Some consumers, particularly children, may require additional legislative protection of their interests in this data. Although companies and governments struggle to protect their intellectual property assets against attacks, sometimes, they may do so at the expense
of other social interests.

1. Information Security and Consumer Data as a Corporate Intangible Asset

Elizabeth Rowe, Greg Vetter and Peter Yu discuss various aspects of the intersection of intellectual property law and data security, specifically raising questions regarding the level of understanding that the corporations and the United States Patent and Trademark Office (USPTO) have of the impact of intellectual property law on information security.

Professor Elizabeth Rowe from the University of Florida School of Law discusses the risks of trade secret loss that companies face if they have weak information security. Through a series of examples of companies that have lost trade secret protection of their key assets, she warns of the danger from rogue insiders because employees present the greatest threat to information security that entities face today.

Professor Greg Vetter from the University of Houston School of Law describes the patentability of cryptographic methodology and its implications. He notes a significant increase in the number of cryptography patents and discusses this increase in the broader historical context of technology patents. Professor Vetter argues that pooling and building portfolios can enable a race to the patent, which can crowd the prior art with the positive and negative effects. Although he says that there is no magic solution to this problem, the evolution of these mechanisms signals possible self-ordering in clearing the patent thicket and license rights that would allow cryptographic technology to move forward in a uniform and standardized way.

Professor Peter Yu from Drake University School of Law presents the international dimensions of intellectual property and information security law. He explains the international political and economic dynamics of information flow and argues that businesses have engaged in regulatory arbitrage by relocating their operations to jurisdictions with more favorable legal environments. To attract foreign investment and retain local businesses, countries now actively participate in a race to the top or the bottom. But, Professor Yu argues, it is important to remember that the reform efforts needed for either race often incur significant costs. By adopting an intellectual property system that ignores the balance between access and protection, countries will ultimately harm their economies by introducing laws that are not tailored to their interest, goals, and local conditions.
2. Information Security and Consumer Data as an Extension of the Individual

Professor Gus Hosein of the London School of Economics cautions us to remain conscious of both pragmatic and principle-based rationales for information security rules. Using an example of the identity card debate in the United Kingdom, he argues in favor of a governmental information security approach that is sensitive to civil liberties. Professor Hosein warns against a balancing test that places security in parity with civil liberties and, therefore, erroneously allows pragmatism to triumph over principle.

C. The Future of Information Security Regulation

Section three addresses two aspects of the future of information security regulation: the development of a common set of corporate information security best practices and the development of workable consumer protection regimes in connection with information security and privacy interests.

1. Establishing Best Practices in Corporate Information Security

Kevin Cronin and Michael Siebecker familiarize us with corporate duties relating to information security and the state of information security litigation in regulatory and technological contexts. They also predict future directions for the development of both the programming code and the law on an international level.

Kevin Cronin, a practicing attorney who has represented clients in data security breach matters before the FTC, presents an overview of the current statutory regime and case law on corporate data care obligations. He cautions that corporate data security cannot exist as an absolute state of impenetrability; rather it is a process of combating internal and external threats on a constant basis. Cronin explains the state of the art in information security case law and discusses possible future legal trends.

Professor Michael Siebecker, an associate professor at the University of Florida Law School, analyzes the role of securities law in connection with the duties of publicly traded companies with regard to information control. Siebecker argues that although the flexibility of evolving common law may be attractive in some contexts, such as Internet regulation, the jurisprudential and practical problems may outweigh the benefits of giving the judges primary responsibility in defining the proper scope of internal data control. Thus, Siebecker asserts that exempting certain small public companies from the certification and audit requirements under Section 404
of SOX is illogical.

2. Building Future Information Security Legal Regimes

Jay Kesan, Jennifer Chandler, Deborah Pierce and Lilian Edwards suggest novel legal approaches to both information security and creation of adequate recourse for individuals and corporations harmed by data breaches. The approaches to re-conceptualization of the balance between legal code and computer code, they argue, may be based on contracts, the Constitution, or involve corporate self-help.

Professor Jay Kesan from the University of Illinois College of Law, in joint work with Ruperto Majuca of the University of Illinois Department of Economics, argue in favor of legal rules that allow “hacking [data] back” in certain business circumstances. They analyze the strategic interaction between the hacker and the attacked company or individual and conclude that neither total prohibition nor unrestrained permission of hack-back is optimal. Instead, they argue that when other alternatives are ineffective, self-defense is the best response to cybercrime because there is a high likelihood of correctly attacking the criminal, and the mitigation of damages to the hacked victim’s systems may outweigh the potential damages to third parties during the hack-back.

Professor Jennifer Chandler from the University of Ottawa School of Law discusses the possibility of contracting around obligations of data security. She views security as a public good that is suffering from a free rider problem. She notes that people tend to consent to contractual terms that impose costs elsewhere. Consistent with this trend, computer owners frequently consent to the terms that impose costs on third parties or the public interest. Professor Chandler argues that to discourage parties from including such terms into contracts, courts should refuse to enforce the terms that externalize security costs.

Deborah Pierce, the executive director of PrivacyActivism, advocates for a Constitutional amendment protecting privacy. She argues that the privacy amendment should protect three types of dignitary interests: (1) dignitary interests with regard to governmentally issued identity documents and private tracking of our activities; (2) individual security and autonomy interests with regard to reproductive rights; and (3) security interest in personal information that affects our ability to act in a self-deterministic way and to defend ourselves against identity theft. For Pierce, privacy should be conceptualized as a fundamental human right that is a necessary component of our notion of liberty: a right that we should be able to assert against both governments and private organizations.
Finally, Professor Lilian Edwards from the University of Sheffield School of Law explores the broader relationship between code based and law based solutions in the context of information security policy. For Professor Edwards, code trumps law: code is generally more effective than regulation at addressing legal or psychological problems. And although the privacy advocate community has been hostile to trusting a computer, she argues that it does not necessarily have to be that way. According to Professor Edwards, some actor in the system needs to have a supervisory role in protecting privacy interests. One way to approach this challenge is to build privacy values into the next generation of trusted computing and have them enforce themselves through code.

In conclusion, these essays strive to create an understandable interdisciplinary voice for the information security debate, bringing together a diverse group of experts to think through ways to improve information security. We hope these thoughts in the nascent legal field of information security and commercial privacy regulation will spur legal conversation, corporate reflection, consumer awareness, and regulatory thoughtfulness in crafting future standards and recourse for harm associated with information security breaches and information crime.

Most importantly, we hope to draw attention to the current critical issues of information vulnerability in our society. Without addressing the issues of information security aggressively and immediately, we risk the viability of our economy, the stability of our markets, and the loss of control over our critical infrastructure systems.