Richmond Journal of Law and Technology

Volume 15 | Issue 4 Article 2

2009

Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets

John T. Soma

J. Zachary Courson

John Cadkin

CORPORATE PRIVACY TREND: THE "VALUE" OF PERSONALLY IDENTIFIABLE INFORMATION ("PII") EQUALS THE "VALUE" OF FINANCIAL ASSETS

By: John T. Soma,[*] J. Zachary Courson,[**] and John Cadkin[***]

Cite as: John T. Soma, et al, *Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets*, XV RICH. J.L. & TECH. 11 (2009), http://law.richmond.edu/jolt/v15i4/article11.pdf.

I. INTRODUCTION

[1] Corporate America's increasing dependence on the electronic use of personally identifiable information ("PII")[1] necessitates a reexamination and expansion of the traditional conception of corporate assets. PII is now a commodity that companies trade and sell.[2] As technological

[*] Professor of Law, University of Denver Sturm College of Law. B.A., Augustana College, 1970; M.A., Economics, University of Illinois, 1973; J.D., University of Illinois, 1973; Ph.D., Economics, University of Illinois, 1975. Executive Director, Privacy Foundation.

[**] B.A., North Carolina State University; J.D. Candidate, 2009, University of Denver Sturm College of Law.

[***] Associate, Townsend and Townsend and Crew, LLP; B.S., University of Wisconsin-Madison, 2000; J.D., University of Denver Sturm College of Law, 2007.

[1] The precise definition of personally identifiable information varies depending upon context. "Personal information" typically encompasses a wide variety of identifiable traits: first and last name, past and present addresses, e-mail addresses, telephone numbers, social security number, gender, birth date, household income, financial and credit account data, medical information, and purchasing history. *See* Will Thomas DeVries, *Protecting Privacy in the Digital Age*, 18 BERKELEY TECH. L.J. 283, 298 (2003).

[2] *See* Corey Ciocchetti, *The Privacy Matrix*, 12 J. TECH. L. & POL'Y 245, 247 (2007)[hereinafter Ciocchetti, *The Privacy Matrix*]; Mark F. Kightlinger, *The Gathering*

development increases, aspects of day-to-day business involving PII are performed electronically in a more cost effective and efficient manner.[3] PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.[4]

[2] There is a catch, however: companies benefiting from the value of PII bear the burden of protecting the privacy interests attached to PII.[5] In light of technological advancement, which often threatens the security of sensitive information,[6] privacy ranks among the most important issues facing modern society.[7] And for good reason, the consumer privacy interest in PII is in a precarious state. Absent adequate safeguards, the building blocks of an individual's virtual identity become increasingly more vulnerable each time the information changes hands.[8] This reality is not lost on American consumers, who are becoming more aware of privacy threats and more skeptical of current levels of privacy safety.[9]

Twilight? Information Privacy on the Internet in the Post-Enlightenment Era, 24 J. MARSHALL J. COMPUTER & INFO. L. 353, 384 (2006).

[3] *See* Jessica M. Lewis, *HIPAA: Demystifying the Implications for Financial Institutions*, 8 N.C. BANKING INST. 141, 141 (2004).

[4] *See* DeVries, *supra* note 1 at 298. ("[I]nstitutions have gradually realized that they sit atop a horde of digital gold: their customers' personal information."). *Id.*

[5] It is important to draw the distinction between privacy and PII from the outset. This article suggests that PII has demonstrable value. Individuals and companies can, among other things, trade, sell, combine and analyze PII. The individual to whom the PII pertains has a privacy interest in the information, specifically the right to control access to their information. The value of privacy is difficult to ascertain.

[6] *See* Janice A. Alwin, *Privacy Planning: Putting the Privacy Statutes To Work for You*, 14 DEPAUL BUS. L.J. 353, 353 (2002); Haeji Hong, *Dismantling the Private Enforcement of the Privacy Act of 1974:* Doe v. Chao, 38 AKRON L. REV. 71, 71 (2005).

[7] Kent Walker, *Where Everybody Knows Your Name: A Pragmatic Look at the Costs of Privacy and the Benefits of Information Exchange*, 2000 STAN. TECH. L. REV. 2, ¶ 1 (citing CHARLES J. SYKES, THE END OF PRIVACY 221 (1999)).

[8] *See* Edmund Mierzwinski, *Privacy Information Sharing and the Boundaries of Each*, B-1473 PLI/CORP. 57, 83 (2005).

[9] Vera Bergelson, *It's Personal but Is It Mine? Toward Property Rights in Personal Information*, 37 U.C. DAVIS L. REV. 379, 428-29 & n.260.

[3] While corporate executives are beginning to realize the importance of data security,[10] the steady rise of data breaches[11] suggests that the groups making internal policy decisions for many of America's companies have yet to grasp or accept a fundamental reality of the modern business world.[12] In order to continue benefiting from the ever-increasing value of PII as an asset, corporate America's leaders must recognize and protect the value of their customers' PII privacy interests in a manner similar to the way they treat and protect financial assets.[13] If companies fail to protect this valuable interest, the backlash from disgruntled consumers and their elected representatives will threaten the access to and use of PII.

[4] Part II of this article explains the basics of privacy, including the definition of informational privacy and the impact of technology. Part III reviews the value of PII to American companies. Part VI assesses the magnitude of the threat to PII, as well as common sources that threaten PII security. Part V covers the most important federal and state privacy regulations in the United States. Part VI analyzes the causes and effects of consumer discontent. Part VII broadly discusses the effects of PII breaches and resulting litigation. Finally, Part VIII makes the case that directors and executives must acknowledge that protection of the privacy interest in PII is now a part of business that must be taken seriously.

[10] Michael L. Rustad & Thomas H. Koenig, *Extending Learned Hand's Negligence Formula to Information Security Breaches*, 3 I/S: J.L. & POL'Y FOR INFO. SOC'Y 237, 238 (2007) (referencing survey of crisis management concerns of corporate executives).
[11] Thomas Claburn, *Record Number of Data Breaches Reported in 2007*, INFO.WEEK, Dec. 31, 2007, http://www.informationweek.com/news/internet/showArticle.jhtml?articleID=205206089 (last visited Mar. 31, 2009) [hereinafter Claburn, *Record Number of Data Breaches*] (reviewing the increase in data breaches from 2006 to 2007).
[12] This contention is by no means novel. Commentaries on this general problem, in varying contexts, can be found in the academic literature. *See generally* Mark F. Foley, *Board Oversight of Information Technology, Data Privacy, and Data Security: Preserving Critical Business Assets*, 80 WIS. LAW. 17, 17 (2007) (offering an expanded analysis of the problem in the specific context of electronic PII).
[13] Jeffrey Taft, *Privacy and Data Security in Service Provider Arrangements: Recent Developments*, 935 PLI/PAT. 485, 491 (2008).

II. PRIVACY BASICS

[5] To understand the imperative of corporate America to provide for the adequate protection of the privacy interest individuals have in their PII, it is necessary to briefly review the traditional views of privacy and the effect of technology in expanding these views. The evolution of the privacy concept places corporate America in a new and unique position as the steward of consumers' virtual identities.

A. A HISTORICAL VIEW OF THE TRADITIONAL CONCEPT OF PRIVACY

[6] While privacy has many faces, the general concept of privacy has existed throughout civilization in diverse cultures.[14] In the American legal community, the right to privacy first found expression as the right against intrusion.[15] While earlier sources express this concept of privacy in varying contexts, the "right to be let alone" entered the American jurisprudential lexicon through the seminal work of Samuel Warren and Justice Louis Brandeis, *The Right to Privacy*.[16] Although their article

[14] Early expressions of the right to privacy are identifiable in Sumerian, Babylonian, Judeo-Christian, and Indian writings. *See, e.g.*, Janet Dean Gertz, Comment, *The Purloined Personality: Consumer Profiling in Financial Services*, 39 SAN DIEGO L. REV. 943, 968 (2002) (discussing aspects of privacy in Mosaic law); *see also* Michael D. Roundy, Note, *The Wiretap Act—Reconcilable Differences: A Framework for Determining the "Interception" of Electronic Communications Following* United States v. Councilman's *Rejection of the Storage/Transit Dichotomy*, 28 W. NEW ENG. L. REV. 403, 405 (2006) (discussing privacy aspects in the Code of Hammurabi).

[15] One of the earliest expressions of the right to privacy in American jurisprudence was echoed in *Wheaton v. Peters*, in which the United States Supreme Court stated "defendant asks nothing—wants nothing, but to be let alone until it can be shown that he has violated the rights of another." Wheaton v. Peters, 33 U.S. 591, 634 (1834). Another early expression of the "right to be let alone" is found in T.M. Cooley's work. THOMAS COOLEY, TREATISE ON THE LAW OF TORTS 389 (rev. students' ed. 1930) ("The new right was conceived of as a right to be let alone—to be free from intrusions into one's own private affairs and from unauthorized publicity concerning one's personal and private affairs.")

[16] Samuel D. Warren and Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 193 (1890):

> Gradually the scope of these legal rights broadened; and now the right to life has come to mean the right to enjoy life, -- *the right to be let alone*; the right to liberty secures the exercise of extensive civil privileges; and the term 'property' has grown to comprise every form of possession -- intangible, as well as tangible.

examined privacy through the lens of tort theory, Brandeis later extended the concept into the constitutional sphere in his dissent in *Olmstead v. United States*.[17] Unlike numerous state constitutions, the United States Constitution does not contain an explicit reference to privacy.[18] It is not surprising, therefore, that the recognition of privacy as a constitutional right by a United States Supreme Court majority opinion did not appear until the mid-1960s.[19] In *Griswold v. Connecticut*,[20] the Court found that the penumbras of the guarantees in the Bill of Rights create zones of privacy.[21] While the methodology of the Court in *Griswold* has been subject to intense criticism,[22] the conclusion that the Constitution protects the right to privacy was groundbreaking and established a basis for extending the right in other contexts.[23] Our traditional view of privacy is premised on the autonomy of the individual and the idea that people should be free from intrusions into their personal lives.

B. RECONCILING PRIVACY WITH TECHNOLOGY

[7] Three major technological developments are transforming our view of privacy: (1) the increase in data creation archiving vast amounts of

---

Id. at 193 (emphasis added).

[17] 277 U.S. 438 (1928). In his dissent in *Olmstead*, Justice Brandeis asserted that the founding fathers "conferred, as against the Government, *the right to be let alone*—the most comprehensive of rights and the right most valued by civilized men." *Id.* at 478 (Brandeis, J., dissenting) (emphasis added). Interestingly, a majority of the Supreme Court of Georgia recognized the right to privacy under the Georgia Constitution ten years before Justice Brandeis's dissent in *Olmstead*. *See* Pavesich v. New England Life Ins. Co., 122 Ga. 190, 197 50 S.E. 68, 71 (Ga. 1905).

[18] For example, Florida's Constitution states, "[e]very natural person has the right to be let alone and free from governmental intrusion into [his] private life except as otherwise provided herein." *E.g.* FLA. CONST. art. I, § 23.

[19] *See* Griswold v. Connecticut, 381 U.S. 479, 515-16 (1965) (holding that a state statute forbidding the use of contraceptives in the marital context violates the right of marital privacy); *see also* Hong, *supra* note 6, at 76 (stating the Court has upheld the right of privacy as a constitutionally protected right in several cases).

[20] 381 U.S. 479 (1965).

[21] *See id.* at 484.

[22] Interestingly, Justice Hugo Black, perhaps the most influential civil libertarian to sit on the Court, adamantly disagreed with the view that the Constitution protects privacy. *See* ROGER K. NEWMAN, HUGO BLACK: A BIOGRAPHY 556-59 (2d ed. 1997).

[23] *See, e.g.*, Roe v. Wade, 410 U.S. 113, 153 (1973) (extending the right to privacy in the abortion context).

personal data; (2) the globalization of data collection and examination; and (3) the lack of adequate control mechanisms for digital information.[24] Due to these developments, the privacy discourse has largely shifted its focus to the right to "informational privacy."[25] Informational privacy is the "claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others."[26]

[8] Informational privacy does not fully equate to the traditional precept of the "right to be let alone."[27] Informational privacy is broader, and more complex, because it reaches beyond the immediate person and into the stream of virtual commerce. Thus, the concept of the "self" in the privacy context is gaining a new and exceedingly more complex meaning.[28] The privacy discourse must now account for cyber or virtual personhood and the new privacy interests this manifestation creates.[29] It is this virtual personality, often voluntarily introduced into virtual commerce by a real person, that individuals now seek to protect from intrusion.[30]

[9] The idea of virtual personality adds a significant third player to privacy security: the data collector and holder.[31] Companies are in the best, and often times only, position to protect PII and the privacy interest

[24] DeVries, *supra* note 1, at 291.
[25] Judith DeCew, *Privacy*, Stanford Encyclopedia of Philosophy, Sept. 18, 2006, http://plato.stanford.edu/ entries/privacy/#InfPri (last visted Mar. 31, 2009); DeVries, *supra* note 1, at 288-91.
[26] Walker, *supra* note 7, ¶ 6 (quoting ALAN F. WESTIN, PRIVACY AND FREEDOM 7 (1967)).
[27] Walker, *supra* note 7, ¶ 5. In fact, "[j]urisprudence has drawn a 'firm line' between 'substantive' ideas of privacy relating to issues affecting personhood and informational ones . . . ." Jonathon W. Penney, *Privacy and the New Virtualism*, 10 YALE J.L. & TECH. 194, 240 (2007) (quoting Sonia K. Katyal, *The New Surveillance*, 54 CASE W. RES. L. REV. 297, 308 (2004)).
[28] *See* COLIN J. BENNETT & CHARLES D. RAAB, THE GOVERNANCE OF PRIVACY: POLICY INSTRUMENTS IN GLOBAL PERSPECTIVE 22 (2003) (discussing the virtual self in the context of Foucalt's notion of panopticon)
[29] *See generally* Penney, *supra* note 27, at 216-29 (discussing personhood in cyberspace).
[30] *See id*. at 225-28.
[31] *See* Walker, *supra* note 7, ¶ 40.

of the individual to whom the information belongs.[32] Because of this unique position, and the extremely difficult task of identifying and capturing identity thieves,[33] companies that deal in PII are becoming increasingly more responsible for the protection of PII.[34] Liability for failing to protect PII from data thieves is a real and present danger for these companies; liability which will increase steadily with the growth of the threat.

III. THE VALUE AND NECESSITY OF ELECTRONIC PII FOR CORPORATE AMERICA

A. NECESSITY

[10] For many companies, the use of paper records has become obsolete.[35] As technology has advanced, corporate America has become dependent upon the electronic storage, transmission, and management of PII.[36] Electronic management of PII is simply faster, cheaper, and easier. The difference in cost between paper and electronic insurance claim processing illustrates the enormous savings the electronic alternative

---

[32] Joshua R. Levenson, Note, *Strength in Numbers: An Examination into the Liability of Corporate Entities for Consumer and Employee Data Breaches*, 19 U. FLA. J.L. & PUB. POL'Y 95, 96 (2008).

[33] The chances of a criminal being caught by federal enforces is one in 700. Chris Jay Hoofnagle, *Identity Theft: Making the Known Unknowns Known*, 21 HARV. J.L. & TECH. 97, 107-08 (2007) (citing AVIVAH LITAN, GARTNER, INC., UNDERREPORTING OF IDENTITY THEFT REWARDS THE THIEVES 1 (2003), http:www.gartner.com/gartner/images/116066.pdf). Obviously, if the resources of the federal government are incapable of successfully tracking down identity thieves, the chances of success for a private plaintiff are exceedingly small.

[34] It is important to point out that a company's duty to protect is not limited to guarding against hackers or stolen laptops. As evidenced by the FTC's treatment of ChoicePoint, discussed *infra* Part VI.B.1, companies are responsible for assuring that the entities with which they do business are legitimate.

[35] *See* Foley, *supra* note 12, at 17-18 (discussing business transitions with reference to technology).

[36] *See* Yves Allain, *The New European Directives on Public Procurement: Change or Continuity?*, 35 PUB. CONT. L.J. 517, 522 (2006); Thomas J. Manley & Scott M. Hobby, *Globalization of Work: Offshore Outsourcing in the IT Age*, 18 EMORY INT'L L. REV. 401, 402 (2004); The Sedona Conference, *Best Practices Commentary on the Use of Search and Information Retrieval Methods in E-Discovery*, 8 SEDONA CONF. J. 189, 192 (2007) [hereinafter The Sedona Conference's *Best Practices Commentary*].

provides.[37] As one commentator points out, the cost of processing an electronic claim is $0.25 to $0.75—a fraction of the $2 to $12 cost of processing the same claim using paper.[38] Managing PII electronically also provides companies with a cost effective outsourcing option, which would be inconceivable if paper were the primary mode of data transfer.[39]

[11] Companies save substantial cost, time, and resources by using electronic data storage instead of physical storage.[40] In the past, companies filed information in bankers' boxes, and then stored the boxes in a warehouse, which might not have been close to a company's office.[41] Today, companies are able to keep the same information in the company's office by storing it electronically on hard drives or other data storage devices.[42] Information that once may have taken days to locate is now available instantaneously.[43] Electronic data storage has also cut the costs of physical transportation and rental space.[44] In addition to these savings, the cost of electronic storage continues to plummet.[45]

B. THE VALUE OF PII

[12] PII is an exceptional resource that companies can use for internal marketing purposes or to sell to other companies.[46] For example, the data points identifying an individual's name and gender would be of little value to the marketing director of a Big & Tall store. But combining that information with weight and height data points would be very valuable to the same marketing director. When a company can identify consumers in its target demographic, its marketing department can efficiently direct advertising resources to that demographic by excluding consumers that

[37] *See* Lewis, *supra* note 3, at 141.
[38] *Id.*
[39] *See* Manley & Hobby, *supra* note 36, at 402.
[40] *See* The Sedona Conference's *Best Practices Commentary*, *supra* note 36, at 192.
[41] *See id.*
[42] *Id.*
[43] *See* Manley & Hobby, *supra* note 36, at 402.
[44] *See* The Sedona Conference's *Best Practices Commentary*, *supra* note 36, at 192.
[45] James X. Dempsey, *Digital Search & Seizure: Updating Privacy Protections to Keep Pace with Technology*, 935 PLI/PAT. 543, 548 (2008). From 1990 to 2007, the storage cost for a typical gigabyte fell from $20,000 to less than $1. The Sedona Conference's *Best Practices Commentary*, *supra* note 33, at 192.
[46] *See* Ciocchetti, *The Privacy Matrix*, *supra* note 2, at 253.

would likely have no interest in the company's product.[47] Here, the benefit to a company using PII is twofold: it raises the probability that advertising will translate into sales, and it cuts the expense of advertising to uninterested consumers.[48]

[13] Another legitimate use of PII enables companies to attract new customers and retain existing customers by offering them the benefits of personalized advertising.[49] And maintaining consumers' personal information "can help both companies and consumers, allowing for more tailored customer service without requiring customers to provide the same information repeatedly."[50] Thus, consumers also benefit from the transparent collection of their personal information.[51]

[14] Due, in part, to the use of PII in marketing decisions, commentators are conceptualizing PII as a commodity.[52] Individual data points have concrete value,[53] which can be traded on what is becoming a burgeoning

---

[47] Corey Ciocchetti, *Just Click Submit: The Collection, Dissemination, and Tagging of Personally Identifying Information*, 10 VAND. J. ENT. & TECH. L. 553, 578-79 (2008) [hereinafter Ciocchett, *Just Click Submit*].

[48] *See* Tal Z. Zarsky, *Desperately Seeking Solutions: Using Implementation-Based Solutions for the Troubles of Information Privacy in the Age of Data Mining and the Internet Society*, 56 ME. L. REV. 13, 37 (2004).

[49] *See* Ciocchetti, *Just Click Submit*, *supra* note 47, at 578-79. (alerting consumers when their favorite product on sale).

[50] Gregory T. Parks & Megan E. Adams, *Can Your Firm Be Sued for a Data Breach*?, E-COMMERCE TIMES, Dec. 8, 2006, http://www.ecommercetimes.com/story/6zyeqfIOat4KEK/Can-Your-Firm-Be-Sued-for-a-Data-Breach.xhtml (last visited Mar. 31, 2009).

[51] *See* Zarsky, *supra* note 48, at 36-37.

[52] *See* Horace E. Anderson, *The Privacy Gambit: Toward a Game Theoretic Approach to International Data Protection*, 9 VAND. J. ENT. & TECH. L. 1, 5 (2006); Grayson Barber, *Personal Information in Government Records: Protecting the Public Interest in Privacy*, 25 ST. LOUIS U. PUB. L. REV. 63, 96 (2006); Ciocchetti, *The Privacy Matrix*, *supra* note 2, at 247; Mark F. Kightlinger, *Twilight of the Idols? EU Internet Privacy and the Post Enlightenment Paradigm*, 14 COLUM. J. EUR. L. 1, 39 (2007); Viktor Mayer-Schonberger, *Beyond Copyright: Managing Information Rights with DRM*, 84 DENV. U. L. REV. 181, 195 (2006).

[53] In 2006, one commentator stated that "a consumer's address can be purchased for 50 cents, an unpublished number for $17.50, a Social Security number for a mere $8, and so on." Luis Salazar, *Part I: Technology Explosion Creates Personal Privacy Tensions*, 25 AM. BANKR. INST. J. 18, 18 (2006). Commenting on the value of information, one commentator has noted, "Even in the manufacturing sectors, the processing of

market for PII.[54] The value of the data increases when combined to provide information, such as consumer preferences that are not discernable from the data points individually.[55] As a result, companies are maintaining, sharing, and selling dossiers of millions of consumer preferences.[56] And as marketing departments become more cognizant of the value of processed information that reveals consumer preferences, the value of this information, along with the PII market, will continue to grow.

[15] PII, if used properly, can generate legitimate profits that require very little input. Further, the ability to maintain PII eliminates the necessity of purchasing PII from another source. But the freedom with which companies currently use PII, and the benefits deriving from such use, is contingent upon the continued acquiescence of consumers and their elected representatives. The potential for increased profits and cost savings serve as a substantial impetus for companies to ensure their actions do not compromise access to this valuable resource.

VI. THE THREAT TO PII

A. THE INCIDENCE OF LARGE SCALE DATA BREACH

[16] The incidence of large data breach is growing at a staggering pace. In 2005, 130 data breaches were reported.[57] This number rose to 315 in 2006, and again to 443 in 2007—an increase of over forty percent in one year.[58] Since 2005, data breaches have compromised over 216 million

information about the goods sold, and about those who purchase and use them, is as important as the production and shipping of the goods themselves." Anderson, *supra* note 52, at 4.

[54] The market for personal information is $1.5 billion annually. Christopher F. Carlton, *The Right to Privacy in Internet Commerce: A Call for New Federal Guidelines and the Creation of an Independent Privacy Commission*, 16 ST. JOHN'S J. LEGAL COMMENT. 393, 405 (2002); Kightlinger, *supra* note 52, at 39.

[55] *See* Zarsky, *supra* note 48, at 37.

[56] Daniel J. Solove, *The Virtues of Knowing Less: Justifying Privacy Protections Against Disclosure*, 53 DUKE L.J. 967, 970 (2003).

[57] Derek A. Bishop, *To Serve and Protect: Do Businesses Have a Legal Duty to Protect Collections of Personal Information?*, 3 SHIDLER J. L. COM. & TECH. 7 (2006) (citing Jon Swartz, *2005 Worst Year for Breaches of Computer Security*, USA TODAY, Dec. 29, 2005, at 1B).

[58] Claburn, *Record Number of Data Breaches*, *supra* note 11.

customer records.[59] In a recent survey of more than 800 privacy professionals, eighty-five percent acknowledged at least one data breach occurred at their company in the past year.[60] Of those same professionals, sixty-three percent acknowledged multiple data breaches over the same period.[61] The statistics for data breaches that translate into actual identity fraud is also a significant concern. From 2005 to 2006, approximately fifteen million Americans fell victim to identity fraud.[62] Perhaps of equal importance, the number of fraud cases during this period rose over fifty percent from the number of cases in 2003.[63]

[17] In the past three years, entities that have suffered a data breach vary from universities to financial institutions. From January 2005 through September 2008, no fewer than 200 American universities, representing every region of the country, experienced a data breach.[64] Financial institutions have also been a common target. Financial giants, including CitiFinancial, Bank of America, Wells Fargo, and Wachovia, have all experienced a substantial data breach.[65] Other recognizable companies representing an array of industries that have experienced a data breach include Boeing, MCI, Kaiser Permanente, Kraft Foods, MTV Networks, Advance Auto Parts, Harley Davidson, Inc., AT&T, and Lloyds of London, just to name a few.[66] Additionally, government entities on the

[59] Thomas Claburn, *The Cost of Data Loss Rises*, INFORMATIONWEEK, Nov. 28, 2007, http://www.informationweek.com/news/internet/showArticle.jhtml?articleID=204204152 (last visited Mar. 31, 2009) [hereinafter Claburn, *The Cost of Data Loss Rises*].
[60] *Reportable and Multiple Privacy Breaches Rising at Alarming Rate, According to Deloitte, Ponemon Institute Survey*, PRNEWSWIRE, Dec. 11, 2007, http://www.reuters.com/article/pressRelease/idUS233283+11-Dec-2007+PRN20071211 (last visited Mar. 31, 2009).
[61] *Id.*
[62] Erin Fonté, *Who Should Pay the Price for Identity Theft?*, 54 FED. LAW. 24, 25 (2007).
[63] *Id.*
[64] The universities targeted represent every geographic region; from the University of Florida to the University of Alaska; from the University of San Diego to Harvard University; and all points in between. Privacy Rights Clearinghouse: A Chronology of Data Breaches, http://www.privacyrights.org/ar/ChronDataBreaches.htm#CP (last visited Mar. 30, 2009).
[65] *Id.*; *see* Kathryn E. Picanso, *Protecting Information Security Under a Uniform Data Breach Notification Law*, 75 FORDHAM L. REV. 355, 356 (2006).
[66] Privacy Rights Clearinghouse, *supra* note 64.

federal,[67] state,[68] and local[69] levels have experienced a data breach. These incidents indicate that data breach can occur in any size company, in any region, and in any industry. Failing to protect PII, therefore, is not far removed from financial Russian roulette.

B. SOURCES AND SCOPE OF DATA BREACH

[18] Data breach results from a plethora of sources.[70] The loss of laptops and similar devices is the most common source of data breach, accounting for forty-nine percent of data breaches.[71] Each laptop lost accounts for an extraordinarily large number of compromised files.[72] Between 2005 and 2006, thirty-two million compromised files were attributable to approximately seventy stolen laptops.[73] In May 2006, the theft of a laptop and a computer storage device compromised data on 28.6 million veterans.[74] This trend continued through 2007 and 2008. In September 2007, the loss of a laptop at Gap, Inc. compromised the personal information of 800,000 job applicants.[75] Some months later, in March 2008, the loss of a box of computer tapes at Bank of New York Mellon compromised the personal information of approximately 12.5 million customers.[76] As with data breach in general, breach due to loss of laptops and other equipment is not specific to any particular industry.[77] Incidents

[67] The Internal Revenue Service, the Department of Defense, the Department of Transportation, and the Department of Veterans Affairs suffered breaches. *Id.*
[68] Georgia, Massachusetts, Indiana, Illinois, Wisconsin, and Rhode Island all experienced a breach at some level. *Id.*
[69] School Districts in Beaverton, Oregon and San Diego, California, and the Detroit Water and Sewage Department were also breached. *Id.*
[70] Liisa M. Thomas, *The Emerging Law of Data Security: From Corporate Obligations to Provide Security to Breach Notification Requirements*, 934 PLI/PAT. 357, 368 (2008).
[71] PONEMON INSTITUTE, LLC, 2007 ANNUAL STUDY: U.S. COST OF A DATA BREACH 11 fig.3 (2007) [hereinafter PONEMON INSTITUTE, LLC, 2007 ANNUAL STUDY].
[72] Chad Pinson, *New Legal Frontier: Mass Information Loss and Security Breach*, 11 SMU SCI. & TECH. L. REV. 27, 28 (2007).
[73] *Id.*
[74] Privacy Rights Clearinghouse, *supra* note 64.
[75] *Id.*
[76] This estimate was reached in August 2008, a significant increase from the original estimate of 4.5 million. *Id.*
[77] *Id.*

have occurred in the financial[78] and healthcare sectors,[79] at universities,[80] and at various levels of government.[81]

[19] Third parties or outsourcers, malicious insiders, hacked systems, and malicious codes also create a large number of data breaches.[82] While these incidents are less common than breach due to lost laptops, the aggregate number of records compromised is extremely high.[83] Hackers are particularly troublesome because they can compromise information without detection[84] and are extremely difficult to catch.[85] The scope of data loss that results when a system is breached can be astronomical. To date, the most infamous data breach occurred at TJX Companies, Inc., where hackers compromised ninety-four million credit card and debit card accounts.[86] Other major data breaches caused by hackers have occurred at CardSystems Solutions, Inc. (forty million credit card records were compromised),[87] Monster.com (1.6 million resumes were compromised),[88]

---

[78] Incidents have occurred at CitiFinancial, J.P. Morgan Chase, and Bank of America, just to name a few of the larger players. *Id.*

[79] Incidents have occurred at Aetna and Kaiser Permanente. *Id.*

[80] Among others, incidents have occurred at George Mason University, Montclair State University, and Cornell University. *Id.*

[81] *Id.*, *supra* notes 67-69.

[82] *See* PONEMON INSTITUTE, LLP, 2007 ANNUAL STUDY, *supra* note 71, at 11 fig.3. (illustrating the allocation of the causes of data breach: laptops lost or stolen (49%); third party or outsourcers (16%); malicious insiders (9%); paper records (9%); electronic backup (7%); hacked systems (5%); malicious codes, like malware and spyware (4%); and other (2%)).

[83] *Id.*

[84] *See* G. Martin Bingisser, *Data Privacy and Breach Reporting: Compliance with Various State Laws*, 4 SHIDLER J. L. COM. & TECH. 9, ¶ 24 (2008).

[85] Hoofnagle, *supra* note 33, at 107-08.

[86] Martin H. Bosworth, *TJX To Pay Mastercard $24 Million for Data Breach*, CONSUMERAFFAIRS.COM, Apr. 6, 2008, http://www.consumeraffairs.com/news04/2008/04/tjx_mc.html (last visited Mar. 31, 2009); Jon Swartz, *TJX Data Breach May Involve 94 Million Credit Cards*, USA TODAY.COM, Oct. 24, 2007, http://www.usatoday.com/tech/news/computersecurity/infotheft/2007-10-24-tjx-security-breach_N.htm (last visited Mar. 31, 2009). *See generally* Richard A. Epstein & Thomas P. Brown, *Cybersecurity in the Payment Card Industry*, 75 U. CHI. L. REV. 203 (2008) (providing an expansive analysis of the TJX debacle).

[87] Jonathan Krim & Michael Barbaro, *40 Million Credit Card Numbers Hacked*, WASH. POST, June 18, 2005, at A1.

and TD Ameritrade Holding Corp (contact information for 6.3 million individuals was compromised).[89]

[20] Similarly, malicious insiders can account for massive amounts of compromised data. In 2007, a malicious insider at Fidelity National Information Systems stole 8.5 million customer records.[90] In 2008, a similar event at Countrywide Financial Corp. resulted in two million compromised files.[91]

C. ASSESSING THE PROBLEM

[21] Data breach clearly presents a growing threat for U.S. companies, both in incidence and scope. Perhaps fortunately, however, many of the threats to data security are organic and may be curtailed through strict enforcement of internal data protection policies.[92] In addition, solutions including encryption, spyware and virus detection, and access protocols leverage technology to prevent breach.[93] As corporate America becomes more dependent upon the electronic use of PII, and as the liability costs of failing to protect that information rise, the internal decision makers must accept the reality that PII management and protection demands a greater allocation of company resources.

---

[88] *Job Seekers Compromised by Monster.com Hack*, CONSUMERAFFAIRS.COM, Aug. 22, 2007, http://www.consumeraffairs.com/news04/2007/08/monster_hack.html (last visited Mar. 31, 2009).

[89] Martin H. Bosworth, *Hackers Steal Information on 6.3 Million Ameritrade Customers*, CONSUMERAFFAIRS.COM, Sept. 15, 2007, http://www.consumeraffairs.com/news04/2007/09/ameritrade_hack.html, (last visited Mar. 31, 2009).

[90] Jaikumar Vijayan, *Fidelity National Data Theft Affects 8.5 Million Customers*, PCWORLD, July 27, 2007, http://www.pcworld.com/businesscenter/article/135117/fidelity_national_data_theft_ ffects_85_million_ customers.html (last visited Mar. 31, 2009).

[91] Renae Merle, *Countrywide Says Consumer Data Were Sold*, WASH. POST, Sept. 14, 2008, at F5.

[92] *See* PONEMON INSTITUTE, LLP, 2007 ANNUAL STUDY, *supra* note 71, at 11.

[93] *See* Thomas M. Laudise, *Ten Practical Things To Know About "Sensitive" Data Collection and Protection*, 929 PLI/PAT. 389, 405 (2008).

V. PRIVACY LEGISLATION: THE PUZZLE OF FEDERAL AND STATE SPHERES OF COVERAGE

[22] Currently, privacy regulation in the United States is best described as a haphazard set of industry specific regulations, at both the federal and state level, which frequently overlap and are often contradictory.[94] Congress has approached privacy regulation with sectoral legislation[95] introducing "specific remedies to specific problems."[96] Where gaps exist in this sectoral approach, Congress has delegated authority to the Federal Trade Commission ("FTC") "to enforce privacy policy promises under its general unfair and deceptive practice powers."[97] In contrast, state legislation offers a broad approach to PII regulation, the most significant of which are data breach notification laws.[98] Despite the patchwork nature of current privacy legislation, it is clear that "[t]he trend in the law is toward imposition of more stringent and more detailed baseline requirements for achieving and demonstrating adequate information security for protected information."[99] This trend will translate into potentially debilitating costs for companies that fail to keep up with the required level of information security.

[94] Walker, *supra* note 7, ¶ 118.
[95] Corey A. Ciocchetti, *E-Commerce and Information Privacy: Privacy Policies as Personal Information Protectors*, 44 AM. BUS. L.J. 55, 73 (2007) [hereinafter Ciocchetti, *E-Commerce and Information Privacy*]
[96] *Id.* The U.S. approach contrasts sharply with the approach taken by some of our closest trade partners. For example, the European Union's regulatory approach provides broad statements of privacy "principles to which society must adhere." *Id.* Additionally, U.S. federal and state "statutes have generally been narrow in scope compared to the more 'horizontal' privacy legislation enacted in Canada." Mark S. Hayes, *The Impact of Privacy on Intellectual Property in Canada*, 20 Intell. Prop. J. 67, 69 n.3 (2006).
[97] Ciocchetti, *E-Commerce and Information Privacy*, *supra* note 95, at 73.
[98] *See, e.g.*, N.C. GEN. STAT. § 75-65 (2008).
[99] John B. Kennedy, *A Primer on Key Information Security Laws in the United States*, 934 PLI/PAT. 117, 126 (2008).

A. FEDERAL GOVERNMENT SECTORAL APPROACH

[23] Congress' sectoral approach[100] generally targets four key areas.[101] Three of these areas, concern regulation of private entities, while the fourth concerns regulation of governmental entities.[102] First, the Children's Online Privacy Protection Act of 1998 ("COPPA") covers children under the age of thirteen.[103] Second, the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") applies to health care institutions and providers.[104] Third, the Financial Services Moderation Act, known as the Gramm-Leach-Bliley Act of 1999 ("GLBA") regulates financial institutions.[105]

1. COPPA

[24] COPPA is an expansive piece of legislation. The purpose of COPPA is to prevent unfair and deceptive practices concerning children's PII by prohibiting the unauthorized collection of PII from children under the age of thirteen.[106] Congress enacted COPPA:

> (1) to enhance parental involvement in a child's online activities in order to protect the privacy of children in the

[100] Commentators note that "U.S. privacy laws to date exist in targeted industries, such as the financial and medical and health industries." Taft, *supra* note 13, at 492.
[101] Ciocchetti, *E-Commerce and Information Privacy*, *supra* note 95, at 73-74.
[102] The focus here is on the federal statutory approach to privacy protection as it relates to non-governmental entities. There are other statutory mechanisms enacted for the purpose of protecting privacy that are applicable to governmental entities. *See, e.g.*, Privacy Act of 1974, 5 U.S.C. § 552a (2000) (protecting federal records that contain PII and creating restrictions and requirements for federal agencies with regard to information disclosure); *see also* Driver's Privacy Protection Act, 18 U.S.C. § 2721 (2000) (prohibiting the disclosure and use of State motor vehicle records); Health Insurance Portability and Accountability Act, Pub. L. No. 104-191, 110 Stat. 1936 (1996) (codified as amended in scattered sections of 26 and 42 U.S.C.); E-Government Act of 2002, Pub. L. No. 107-347, 116 Stat. 2899 (codified as amended in scattered sections of 5, 10, 13, 15, 18, 28, 31, 40, 41, and 44 U.S.C.) (requiring government agencies to publish Privacy Impact Assessments).
[103] 15 U.S.C. §§ 6501-6506 (2006).
[104] Pub. L. No. 104-191, 110 Stat. 1936 (1996).
[105] Financial Modernization Act of 1999, 15 U.S.C. §§ 6801-6809 (2006).
[106] Pub. L. No. 105-277, 112 Stat. 2681 (1998); *see also* 144 Cong. Rec. S12741-04 (1998).

> online environment; (2) to enhance parental involvement to help protect the safety of children in online fora such as chatrooms, home pages, and pen-pal services in which children may make public postings of identifying information; (3) to maintain the security of personally identifiable information of children collected online; and (4) to protect children's privacy by limiting the collection of personal information from children without parental consent.[107]

2. HIPAA

[25] In 1996, Congress attempted to standardize privacy concerning health care information with HIPAA.[108] To foster efficiency, HIPAA requires the standardization of electronic data interchange in healthcare delivery.[109] HIPPA also addresses the confidentiality and security of health data by setting standards and the means of enforcing those standards.[110] The legislation requires the Department of Health and Human Services to publish new rules that will ensure "[s]tandardization of electronic patient health, administrative and financial data," "[u]nique health identifiers for individuals, employers, health plans and health care providers," and "[s]ecurity standards protecting the confidentiality and integrity of 'individually identifiable health information,' past, present and future."[111]

3. GLBA

[26] As HIPAA protects health information, GLBA protects financial information.[112] GLBA imposes new requirements and rules on financial

---

[107] Janine Hiller et al., *Pocket Protection*, 45 AM. BUS. L.J. 417, 428 (2008) (citing 144 Cong. Rec. S12741-04 (1998) (remarks of Sen. Bryan)).
[108] HIPAA, Whatis.com, http://searchcio.techtarget.com/sDefinition/0,,sid19_gci862786,00.html (last visited Mar. 31, 2009).
[109] Vox2Data: Electronic Health Record and Voice Activated Transcription Software for Physicians, http://www.vox2data.com/faqs.html (last visited Mar. 31, 2009).
[110] *Id.*
[111] *Id.*
[112] *See* Anthony Rollo, *The New New Litigation Thing: Consumer Privacy*, 1301 PLI/CORP. 9, 27 (2002).

institutions, including: requirements to protect personal financial information of customers, restrictions on disclosure to non-affiliate third parties, requirements to disclose security and privacy policies to consumers, and prohibitions of the use of fraudulent means to obtain financial information.[113] Importantly, GLBA contained new privacy regulations to protect financial "nonpublic personal information."[114]

B. DATA BREACH NOTIFICATION LAWS

[27] Following a general trend of information disclosure,[115] commentators and legislatures turned their attention to laws requiring companies to disclose data security breaches shortly after the turn of the millennium. The approach of data breach notification laws differs from the sectoral approach in two principal respects. First, where the sectoral approach provides comprehensive regulation, including preventative requirements, data breach notification regulation concerns post-breach requirements.[116] Second, data breach notification laws generally transcend the limited approach of addressing individual sectors by focusing broadly on all entities that store or maintain PII.[117]

[113] GLBA extends beyond what would traditionally be considered a financial institution. "Among the institutions that fall under FTC jurisdiction for purposes of the GLB Act are non-bank mortgage lenders, loan brokers, some financial or investment advisers, tax preparers, providers of real estate settlement services, and debt collectors." Federal Trade Commission, In Brief: The Financial Privacy Requirements of the Graham-Leach-Bliley Act, http://www.ftc.gov/bcp/edu/pubs/business/idtheft/bus53.pdf.
[114] DeVries, *supra* note 1, at 299 (citing 15 U.S.C. § 6801(a) (2006)).
[115] *See* Paul M. Schwartz & Edward J. Janger, *Notification of Data Security Breaches*, 105 MICH. L. REV. 913, 916 (2007). Professors Schwartz and Janger provide the following examples of other information disclosure requirements: mandates that hospitals "publicize performance results for certain medical procedures," mandates that manufacturers affix energy efficiency labels to products, and mandates that companies report workplace injuries. *Id.* at 915. Cass Sunstein coined the term "regulation through disclosure" to describe this trend. *Id.* (quoting Cass R. Sunstein, *Information Regulation and Information Standing: Akins and Beyond*, 147 U. PA. L. REV. 613, 613 (1999)).
[116] *Compare* 15 U.S.C. § 6801(a) (2006) (regulating financial institutions) *with* N.C. GEN. STAT. § 75-65 (2008) (affecting any business that "owns or licenses personal information").
[117] *See, e.g.*, N.C. GEN. STAT. § 75-65 (2008).

[28] While numerous data breach notification bills have been introduced,[118] there is currently no broad-based federal data breach notification legislation.[119] Further, it is questionable if the bills now before Congress will become law.[120] As consumers become more conscious of the precarious state of their privacy interests in their PII, and companies become overwhelmed by the difficulties of complying with numerous state laws, it is reasonable to assume that Congress will enact federal legislation to bring consistency to the area of data breach notification law.

[29] While a federal law is lacking, forty-four states, as well as the District of Columbia and Puerto Rico, have enacted data breach notification legislation.[121] State data breach notification laws generally require companies to inform customers when a data breach affecting consumer information occurs.[122] In most states, any entity that owns, licenses, or maintains PII belonging to a citizen of that state falls under the

[118] Brandon Faulkner, Note, *Hacking into Data Breach Notification Laws*, 59 FLA. L. REV. 1097, 1114, 1114 nn.115 & 117 (2007) (citing numerous bills introduced during the 109th and 110th Congresses); *see also Senate Vote on Data Brokers Likely This Week*, CONSUMERAFFAIRS.COM, Sept. 25, 2006, http://www.consumeraffairs.com/news04/2005/senate_data_privacy.html (last visited Mar. 31, 2009).

[119] Kristan T. Cheng, *Identity Theft and the Case for a National Credit Report Freeze Law*, 12 N.C. BANKING INST. 239, 269-70 (2008); *see* James T. Graves, Note, *Minnesota's PCI Law: A Small Step on the Path to a Statutory Duty of Data Security Due Care*, 34 WM. MITCHELL L. REV. 1115, 1120 (2008). One commentator has opined that the lack of a federal law reflects "growing concerns that most of the bills would take a step backward from existing state laws." Vinita Bali, *Data Privacy, Data Piracy: Can India Provide Adequate Protection for Electronically Transferred Data?*, 21 TEMP. INT'L & COMP. L.J. 103, 115 (2007).

[120] Kennedy, *supra* note 99, at 209.

[121] *See* National Conference of State Legislatures, State Security Breach Notification Laws, http://www.ncsl.org/ programs/lis/cip/priv/breachlaws.htm (last visited Mar. 31, 2009). Alaska, Arizona, Arkansas, California, Colorado, Connecticut, Delaware, Florida, Georgia, Hawaii, Idaho, Illinois, Indiana, Iowa, Kansas, Louisiana, Maine, Maryland, Massachusetts, Michigan, Minnesota, Montana, Nebraska, Nevada, New Hampshire, New Jersey, New York, North Carolina, North Dakota, Ohio, Oregon, Pennsylvania, Rhode Island, South Carolina, Tennessee, Texas, Utah, Vermont, Virginia, Washington, West Virginia, Wisconsin, and Wyoming have data breach notification laws. *Id.*

[122] *See, e.g.*, ARIZ. REV. STAT. ANN. § 44-7501 (2009); *see also* MICH. COMP. LAWS § 445.72 (2007).

statutory purview.[123] State laws differ, to a degree, on the types of actions triggering the duty to disclose. Some states require disclosure upon breach, while other states require disclosure when, after internal investigation, PII is believed to have been compromised.[124] In addition, most state laws do not require disclosure if it was encrypted data that was lost.[125]

C. THE IMPLICATIONS FOR CORPORATE AMERICA

[30] The cost of failing to comply with federal privacy regulation warrants the attention of corporate America.[126] HIPAA, for example, provides for civil and criminal penalties.[127] Failure to comply with HIPAA's requirements creates civil "penalties of $100 per violation, up to $25,000 per year."[128] Criminal sanctions, however, are much more severe, reaching up to $250,000 in fines and ten years in prison.[129] While COPPA does not carry criminal penalties,[130] the FTC sent companies a clear message that violations of COPPA will receive severe treatment.[131] In 2006, the FTC pursued Xanga.com for COPPA violations; the controversy ended in a settlement agreement that required Xanga.com to "pay a $1 million fine, implement policies compliant with COPPA, file additional

[123] *See, e.g.*, COLO. REV. STAT. § 6-1-716(2)(a)-(b) (2009); *see also* N.C. GEN. STAT. § 75-65 (2008).
[124] *Compare* ARIZ. REV. STAT. ANN. § 44-7501 (2009) (requiring notification after a breach), *with* CONN. GEN. STAT. § 36a-701b (2009) (not requiring notification after a breach if a reasonable determination is made "that the breach will not likely result in harm to the individuals whose personal information has been acquired and accessed").
[125] *See, e.g.*, IND. CODE ANN. §24-4.9-3-3 (2008).
[126] Foley, *supra* note 12, at 18 ("Noncompliance with regulatory schemes may result in orders prohibiting data use or other practices, civil or criminal fines, imprisonment for managers and directors, or decades-long oversight by regulatory agencies.").
[127] American Medical Association, HIPAA Violations and Enforcement, http://www.ama-assn.org/ama/pub/category/11805.html (last visited Mar. 31, 2009) (discussing HIPAA violations pursuant to 42 U.S.C. § 1320d-2 (2006)).
[128] *Id.; see* Lewis, *supra* note 3, at 141-42.
[129] American Medical Association, *supra* note 119.
[130] *See* 15 U.S.C. §§ 6501-6506 (2006).
[131] *See* Hiller et al., *supra* note 107, at 418 ("The FTC fine against Xanga was the largest ever imposed under COPPA.")

status reports, and submit to monitoring by the FTC."[132] These examples are just the beginning. As the threat to PII grows, so will the breadth of statutory coverage and consequences of failing to adhere to federal mandates.

[31] The costs associated with state regulation may be even more substantial.[133] Depending upon the amount of information compromised, the process of data breach notification can create substantial costs.[134] A 2007 study estimates that notification of data breach costs $15 per record.[135] Providing notification for breaches similar in scale to those sustained by TJX[136] or CardSystems[137] could result in costs that would prove debilitating to many U.S. companies. The challenge of adhering to the different notification requirements of different state statutes adds significant strategic obstacles, and failure to provide adequate notification can create additional costs. For example, under Florida's data breach notification statute, a company may be liable "[i]n the amount of $1,000 for each day the breach goes undisclosed for up to 30 days and, thereafter, $50,000 for each 30-day period or portion thereof for up to 180 days."[138] Furthermore, companies that do not disclose within 180 days may be

[132] *Id.* (citing Press Release, Federal Trade Commission, Xanga.com To Pay $1 Million to Violating Children's Online Privacy Protection Rule (Sept. 7, 2006) *available at* http://www.ftc.gov/opa/2006/09/xanga.shtm).
[133] *See, e.g.*, Kennedy, *supra* note 99, at 185 (noting that "[i]n addition to state Attorney Generals, other state agencies have sometimes been involved in the enforcement of their state's breach notification laws.").
[134] *See* Ellen Messmer, *TJX Lists Mounting Costs of Data-Breach Debacle*, NETWORK WORLD, June 8, 2007, http://www.networkworld.com/news/2007/060807-tjx.html (last visited Mar. 31, 2009) ("In its quarterly filing with the Securities and Exchange Commission, TJX acknowledged that the computer intrusion . . . cost it $20 million during the first quarter alone, and that costs were expected to continue to mount in future quarters.").
[135] PONEMON INSTITUTE, LLC, 2007 ANNUAL STUDY, *supra* note 71, at 9.
[136] *See* Bosworth, *TJX To Pay Mastercard $24 Million for Data Breach*, *supra* note 86; Swartz, *supra* note 86.
[137] *See* Krim & Barbaro, *supra* note 87.
[138] FLA. STAT. § 817.5681(b)(1) (2008).

subject to "an administrative fine of up to $500,000"[139] and the cost of failing to notify increases with each state statute that is implicated.[140]

[32] While the fines resulting from noncompliance with privacy legislation, and the cost associated with providing data breach notification are substantial, the prospect of tighter, more comprehensive regulation may be even more daunting. Companies obviously have a significant interest in crafting their own data protection protocols.[141] But if the high incidence of data breach continues, governmental bodies may find it necessary to enact legislation that will impose broader and more burdensome requirements for data protection. More concerning is the fact that legislatures may create laws restricting the ability of companies to access, store, use, and transfer electronic data.[142] To prevent the enactment of legislative measures of this type, companies must take it upon themselves to reduce the incidence of data breach by proactively creating internal measures that effectively provide for the protection of PII.

VI. PRIVACY LAWSUITS

A. PRIVATE SUITS

[33] Some commentators argue that traditional tort doctrines adequately protect against harms caused by loss or misuse of personal information.[143]

---

[139] FLA. STAT. § 817.5681(b)(2) (2008).

[140] S*ee* Kirk J. Nahra, *New State Information-Security Requirements Challenge Business*, PRIVACY IN FOCUS, Nov. 2008, at 1, http://www.wileyrein.com/docs/newsletter_issues/622.pdf.

[141] *See id.*, at 2, 4, 5.

[142] *See* Willkie Farr & Gallagher LLP, *Recent State Data Privacy Laws and Court Decisions Impose Extensive Obligations on Companies that Collect and Process Personal Information*, Oct. 10, 2008, http://www.willkie.com/files/tbl_s29Publications%5CFileUpload5686%5C2732%5CRecent_State_Data_Privacy_Laws.pdf ("Companies doing business in [] states must carefully review these new requirements and develop and implement compliance procedures to protect adequately the nonpublic personal information they collect, store, and distribute.").

[143] *See* Walker, *supra* note 7, ¶ 171 (noting that "[c]onsumers can already sue a company whose system was hacked" and that "private sector enforcement . . . is the real enforcement mechanism for meaningful security").

Currently, however, the bridge between traditional tort and privacy law is incomplete.[144] Many potential lawsuits are never filed because the market or judicial valuation of an individual's PII is not sufficiently high to offset the cost of litigation.[145] Further, as damages are usually difficult to prove, even a verdict for the plaintiff does not guarantee an award of damages.[146]

[34] But, certain political and legislative developments indicate that the climate could soon change.[147] Proposed theories for extending liability for data breach to companies holding PII already exist in academic literature.[148] It is likely only a matter of time before courts begin to adopt similar theories of liability and common law standards emerge.[149] Companies will have to defend against lawsuits brought by individuals harmed by data breach and financial institutions that incur costs due to data breach.[150] Minnesota has already enacted a statute that allows financial institutions to pursue retailers and merchants for costs incurred due to data breach,[151] and similar legislation is pending in other states.[152]

---

[144] *See* Paul M. Schwartz, *Spyware: The Latest Cyber-Regulatory Challenge: Privacy and Inalienability and the Regulation of Spyware*, 20 BERKELEY TECH. L.J. 1269, 1275 (2005)

[145] *See* Walker, *supra* note 7, ¶¶ 168, 178; Schwartz, *supra* note 144, at 1275.

[146] Schwartz, *supra* note 144, at 1275; Levenson, *supra* note 32, at 102.

[147] *See* Parks & Adams, *supra* note 50 ("Congress and state legislatures have begun considering new laws relating to data privacy and security.").

[148] *See* Jennifer A. Chandler, *Negligence Liability for Breaches of Data Security*, 23 BANKING & FIN. L. REV. 223, 225 (2008) (addressing "the possibility of using liability in negligence as a means to deter unreasonably careless data security practices as well as to offer compensation to those harmed by data security breaches."); Meiring de Villiers, *Reasonable Foreseeability in Information Security Law: A Forensic Analysis*, 30 HASTINGS COMM. & ENT. L.J. 419, 420 (2008) (presenting "an analysis of civil liability for failure to safeguard confidential information."); Levenson, *supra* note 32, at 97 (finding "a legal cause of action for a breach of contract against a corporation that aggregates personally identifiable information"); Rustad & Koenig, *supra* note 10, at 237 (arguing "that Learned Hand's famous risk/utility test should be extended to create a duty to secure computer systems applicable against companies that hold sensitive personal information").

[149] *See, e.g.*, Am. Bankers Ass'n v. Lockyer, 541 F.3d 1214, 1218 (9th Cir. 2008) (holding that California's Financial Information Privacy Act was not preempted by the Federal Fair Credit Reporting Act).

[150] *See* Bosworth, *TJX To Pay Mastercard $24 Million for Data Breach*, *supra* note 86; Swartz, *supra* note 86.

[151] *See* Kennedy, *supra* note 99, at 186 (citing MINN. STAT. § 325E.64 (2008)).

Once this occurs, the extension of liability will develop rapidly from jurisdiction to jurisdiction.

[35] As noted above, state laws that create a right of action for financial institutions are emerging.[153] The settlements between TJX and financial institutions that incurred losses due to the TJX breach illustrate the magnitude of the costs companies may incur by failing to protect PII.[154] By mid-2008, TJX had spent tens of millions of dollars settling with financial institutions, including a $24 million settlement with MasterCard and its issuing lenders,[155] and a larger $40.9 million settlement with Visa.[156] These settlements are likely to embolden financial institutions in the future to take PII security seriously, thereby increasing the liability of companies that fail to follow suit.

B. GOVERNMENT LAWSUITS

1. FEDERAL ENFORCEMENT

[36] The Federal Trade Commission ("FTC") has the authority to fill in the gaps left by Congress's sectoral approach.[157] Initially, the FTC suggested that industry self-regulation offered the best defense of online

---

[152] *Id.* at 186-87 (noting that similar legislation to Minnesota's statute is also pending in Texas, Illinois, Michigan, Washington, and Massachusetts).

[153] *See supra* notes 150-52 and accompanying text. As Attorney John Kennedy of Dewey & LeBoeuf notes, "[t]hese statutes reverse court decisions that came in the wake of the breach at BJ's Warehouse in which courts dismissed all claims against BJ's by banks that had to replace payment cards following the theft of customer card data from BJ's." Kennedy, *supra* note 99, at 187.

[154] *See* Bosworth, *TJX To Pay Mastercard $24 Million for Data Breach*, *supra* note 86; Swartz, *supra* note 86.

[155] Linda McGlasson, *TJX, MasterCard Agree on $24 Million Settlement: Institutions Have 90 Days to Approve Deal in Data Breach Case,* BANK INFO SECURITY, Apr. 4, 2008, http://www.bankinfosecurity.com/articles. php?art_id=811 (last visited Mar. 31, 2009); Bosworth, *TJX To Pay Mastercard $24 Million for Data Breach*, *supra* note 86.

[156] Mark Jewell, *TJX, Visa Reach $40.9M Settlement for Data Breach*, USA TODAY, Nov. 30, 2007, http:// www.usatoday.com/money/industries/retail/2007-11-30-tjx-visa-breach-settlement_N.htm (last visited Mar. 31, 2009); *see* Mark Huffman, *TJX Settles Visa Suit Over Data Breach*, CONSUMERAFFAIRS.COM, Nov. 30, 2007, http://www. consumeraffairs.com/news04/2007/11/tjx_visa.html (last visited Mar. 31, 2009).

[157] *See* Ciocchetti, *E-Commerce and Information Privacy*, *supra* note 95, at 73.

privacy.[158] Not long after taking this position, however, the FTC performed an about-face, recognizing that industry self-regulation had fallen short of its goals.[159] After reevaluating the necessity of its involvement, the FTC asserted itself as a major player in the pursuit of privacy violations.

[37] In 2000, the FTC trained its sights on the ad-serving company, DoubleClick.[160] Privacy alarms sounded when DoubleClick announced its intention to acquire Abacus Corp., a business that used traditional direct marketing and had a massive database of consumer PII.[161] The pairing of these two companies could have led to very extensive and detailed profiles of Internet users.[162] The FTC initiated its investigation based on a complaint that DoubleClick had engaged in unfair and deceptive trade practices by tracking online activities of Internet users and combining that data with detailed PII contained in a separate national marketing database.[163] DoubleClick placed "cookies" in banner advertisements on WebPages.[164] Clicking on these banner ads would redirect the Internet browser to a DoubleClick server.[165] This permitted DoubleClick to create

[158] *See* FEDERAL TRADE COMMISSION, SELF-REGULATION AND PRIVACY ONLINE 6 (1999), *available at* http://www.ftc.gov/os/1999/07/privacy99.pdf.
[159] *See* FEDERAL TRADE COMMISSION, PRIVACY ONLINE: FAIR INFORMATION PRACTICES IN ELECTRONIC MARKETPLACE, at ii-iii (2000), *available at* http://www.ftc.gov/reports/privacy2000/privacy2000.pdf.
[160] *See* Linda A. Goldstein, *Consumer Privacy Online: Recent Trends and Updates*, 748 PLI/PAT. 1145, 1161 (2003); Ira S. Rubinstein et al., *Data Mining and Internet Profiling: Emerging Regulatory and Technological Approaches*, 75 U. CHI. L. REV. 261, 271 (2008).
[161] Rubinstein et al., *supra* note 160, at 271; Seth Richard Lesser, *Privacy Law in the Internet Era: New Developments and Directions*, 701 PLI/PAT. 115, 123 (2002).
[162] *See* Frederic Debusseré, *The EU E-Privacy Directive: A Monstrous Attempt to Starve the Cookie Monster?*, 13 INT'L J.L. & INFO. TECH. 70, 71 (2005).
[163] *See* Lesser, *supra* note 161, at 121-22.
[164] Ciocchetti, *The Privacy Matrix*, *supra* note 2, at 257, 257 n.32 (citing Marshall Brain, *How Internet Cookies Work*, HOWSTUFFWORKS.COM, http://www.howstuffworks.com/cookie.htm (last visited Mar. 31, 2009)).
[165] Lesser, *supra* note 161, at 121-22; *see* Ken Dreifach, *Data Privacy, Web Security, and Attorney General and FTC Enforcement*, 902 PLI/PAT. 207, 224 (2007).

profiles about users and their Internet surfing habits.[166] Concern over the possibility of privacy intrusion led to multiple state and federal lawsuits.[167]

[38] In the end, the court consolidated these suits, and DoubleClick settled.[168] The terms of the settlement required DoubleClick to: (1) create an easy to read privacy policy, which outlines the company's use of cookies and pixel tags, and explains its online advertising service; (2) launch 300 million banner advertisements on sites across the internet that explain how consumers can protect their privacy, opt out of having a DoubleClick advertisement server cookie placed on their computers, and how cookies are used and data is collected; (3) purge user information that the company collected on consumers on a regular basis; (4) hire an accounting firm to audit its compliance with the terms; and (5) pay $1.8 million in attorneys' fees.[169]

[39] The FTC obtained another large privacy-related settlement from the data broker ChoicePoint.[170] ChoicePoint compiled and sold PII.[171] In 2005, the company announced that it sold information to people who turned out to be identity thieves.[172] The FTC charged ChoicePoint with violating the "Fair Credit Reporting Act (FCRA) by furnishing consumer reports – credit histories – to subscribers who did not have a permissible purpose to obtain them, and by failing to maintain reasonable procedures to verify both [subscriber] identities and how [the subscriber's] intended to use the information."[173] The FTC reached a settlement with ChoicePoint,

---

[166] Lesser, *supra* note 161, at 122; *see* Ian Rambarran & Robert Hunt, *Are Browse-Wrap Agreements All They Are Wrapped Up To Be?*, 9 TUL. J. TECH. & INTELL. PROP. 173, 198-99 (2007).

[167] Drefifach, *supra* note 165, at 223; Lesser, *supra* note 161, at 123-24.

[168] Brian Sullivan, *Privacy Groups Debate DoubleClick Settlement*, CNN.COM, May 24, 2002, http://archives.cnn.com/2002/TECH/internet/05/24/doubleclick.settlement.idg/index.html (last visited Mar. 31, 2009).

[169] *Id.*

[170] *See* Kennedy, *supra* note 99, at 158.

[171] Federal Trade Commission, Federal Trade Commission's Settlement with ChoicePoint, http://www.ftc.gov/choicepoint (last visited Mar. 31, 2009) [hereinafter FTC Settlement].

[172] *Id.*

[173] Press Release, Federal Trade Commission, ChoicePoint Settles Data Security Breach Charges; to Pay $10 Million in Civil Penalties, $5 Million for Consumer Redress (Jan.

requiring the company to pay $5 million to reimburse consumers for expenses due to identity theft.[174] ChoicePoint also agreed to pay $10 million in civil penalties[175] and implement new procedures to ensure that consumer reports are provided to only "legitimate businesses for lawful purposes, to establish and maintain a comprehensive information security program, and to obtain audits by an independent third party security professional every other year until 2026."[176] Not only must the company pay for an independent third party review, but if the review is not up to FTC standards, the FTC could potentially reopen the settlement until 2026.

2. STATE ENFORCEMENT

[40] In addition to the FTC, state attorney generals can bring significant privacy lawsuits against companies.[177] In *Hatch v. U.S. Bank, N.A.*,[178] U.S. Bank sold customer information, including checking account and credit card numbers, account activity information, marital status, gender, social security numbers, bankruptcy scores, and other information, to telemarketing firms for more than $4 million.[179] Minnesota's attorney general filed suit against U.S. Bank for consumer fraud, false advertising, deceptive trade practices, and state common law privacy problems in connection with sales of bank customer's private information.[180] The bank quickly settled, agreeing to: inform customers of its privacy policy and provide customers the ability to opt out of sharing information with affiliated organizations, make refunds to customers who purchased services and were not happy, and pay a substantial settlement.[181] Ultimately, the settlement amount reached $4 million dollars.[182]

26, 2006) *available at* http://www.ftc.gov/opa/2006/01/choicepoint.htm [hereinafter Press Release, FTC]

[174] *Id.*; *see* FTC Settlement, *supra* note 171.

[175] Press Release, FTC, *supra* note 173.

[176] *Id.*

[177] *See* Hiller et al., *supra* note 107, at 418

[178] Hatch v. U.S. Bank N.A., No. 99-872 (D. Minn. Sep. 25, 2000) (order granting injunctive and consumer relief).

[179] Rollo, *supra* note 112, at 45-46.

[180] *Id.* at 45.

[181] *Id.* at 46; *see* Robert Gellman, *Privacy, Consumers and Costs: How the Lack of Privacy Costs Consumers and Why Business Studies of Privacy Costs Are Biased and*

[41] In New York, attorney general Eliot Spitzer sued Chase Manhattan Bank ("Chase") for sharing its cardholders' personal information with third party marketers without first disclosing this sharing to its customers.[183] The state reached a settlement with the bank that provided significant privacy protection for New York customers, exceeding the protections provided by the GLBA.[184] Chase altered privacy policies by ceasing to share PII with unaffiliated third parties, and only shared names, addresses, and phone numbers with affiliates.[185] Customers could also opt out of any information sharing.[186] In addition to agreeing to refrain from sharing consumer's personal financial information, Chase paid attorneys fees in the amount of $101,500 to the attorney general.[187]

VII. THE CONSUMER EFFECT

[42] As discussed above, state legislatures are increasing their regulatory roles in protecting PII, and Congress is likely to follow. The FTC and state attorney generals are similarly increasing their presence and consumers are exerting a corresponding pressure that companies are

Incomplete, Mar. 2002, http://epic.org/reports/dmfprivacy.html (last visited Mar. 31, 2009).

[182] David Annecharico, *Online Transactions: Squaring the Gramm-Leach-Bliley Act Privacy Provisions with the FTC Fair Information Practice Principles*, 6 N.C. BANKING INST. 637, 640-41 (2002).

[183] Press Release, Office of NewYork State Attorney Gen. Eliot Spitzer, Spitzer Secures Privacy Agreement with National Bank, Jan. 25, 2000, *available at* http://www.oag.state.ny.us/media_center/2000/jan/jan25b_00.html [hereinafter N.Y. Press Release].

[184] Rollo, *supra* note 112, at 47.

[185] *Id.*

[186] *Id.*

[187] N.Y. Press Release, *supra* note 183. One other example of the *Fidelity* case: The Electronic Privacy Information Center (EPIC) filed amicus briefs against Fidelity Federal Bank for buying more than half a million names and addresses from the Florida Department of Highway Safety and Motor Vehicles. EPIC argued that Fidelity, valued at $4 billion, bought 565,600 names and addresses, and claimed that the purchase violated the Drivers Privacy Protection Act. The court ordered Fidelity to pay $50 million in settlement. *See* K.C. Jones, *Bank To Pay $50 Million for Buying Personal Data*, FINANCETECH, Sept. 30, 2006, http://financetech.com/news/showArticle.jhtml;jsessionid=0GITFOLJTPWYQQSNDLPSKHSCJUNN2JVN?articleID=193005173 (last visited Mar. 31, 2009).

beginning to feel.[188] As the public becomes more conscious of the precarious state of consumer privacy interest in their PII, consumer pressure on businesses will increase proportionately. Soon, businesses may face the choice of either proactively protecting their consumer's PII or losing their customer base.

A. THE IMPETUS FOR CONSUMER ACTION

[43] In 2005, approximately twelve percent of nine thousand consumers surveyed had received notification regarding a breach of their PII.[189] Of these breaches, eighty-six percent involved the loss or theft of consumer information, while the remaining fourteen percent involved employee, student, medical, and taxpayer data.[190]

[44] In 2006, the cost of fraud was an estimated at $55.7 billion.[191] Victims of privacy breach and identify theft "estimate[d] the total value of all charges on fraudulent accounts in their name" at $87,303 on average.[192] Individual consumer estimates ranged from $50 to $500,000 per act, and the average estimate loss to business creditors due to fraud have increased seventy-eight percent since 2004.[193] Furthermore, resolution of privacy breaches takes the consumer significant time and funding. While it is estimated that the consumer spends ninety-seven hours to repair the damage when an existing account has been used to affect fraud, if a new account has been created in the victim's name, resolution of the breach skyrockets to 231 hours.[194] In 2006, the average consumer's out-of-pocket costs to resolve breaches for existing or new accounts averaged $1,884 and $1,342 respectively.[195] Not surprisingly, "theft or loss of personal and

[188] *See* PONEMON INSTITUTE, LLC, 2007 ANNUAL STUDY, *supra* note 71, at 3, 10, 13.
[189] PONEMON INSTITUTE, LLC, NATIONAL SURVEY ON DATA SECURITY BREACH NOTIFICATION 2 (2005).
[190] *Id*. at 3.
[191] Fonté, *supra* note 62, at 25.
[192] IDENTITY THEFT RESOURCE CENTER, IDENTITY THEFT: THE AFTERMATH 2006, at 15 (2007).
[193] *Id.*
[194] *Id.* at 3.
[195] *Id.*

financial information is the No. 1 concern of consumers worldwide (64 percent)."[196]

B. THE COST OF LOST CONSUMER CONFIDENCE

[45] Loss of customer information can have detrimental effects on businesses, and a reduction in consumer confidence may translate to a reduction in future revenue.[197] Repeated instances of personal information security breaches will likely have a negative impact on a corporation's customer base.[198] Specifically, in response to receiving two or more notifications of a privacy breach, most customers would take their business elsewhere.[199] Further, breaches diminish the potential for bringing in new customers.[200] Given the astonishingly high rate of security lapses, it is clear that the impact on corporate goodwill and brand image is a "strategic risk that requires the attention of senior management."[201]

[46] A recent study suggests that loss of goodwill results in quantifiable financial harm.[202] The Ponemon Institute suggests privacy breaches "translate[] to lost business opportunity."[203] Lost opportunity is measured through "customer churn and acquisition costs," which have risen "from $98 per record in 2006 to $128 in 2007 – a [thirty percent] increase."[204] The impact of this upward trend cannot be overemphasized. As consumer awareness increases, the rate of consumer turnover will likely follow.

---

[196] Press Release, Visa Inc., Technology, Cross-Industry Collaboration Key to Enhancing Data Security (Jan. 25, 2006), *available at* http://www.corporate.visa.com/md/nr/press280.jsp.
[197] PONEMON INSTITUTE, LLC, 2006 ANNUAL STUDY: COST OF A DATA BREACH 5 (2006) [hereinafter PONEMON INSTITUTE, LLC, 2006 ANNUAL STUDY].
[198] The Ponemon Institute identifies this as customer churning: "[t]he estimated number of customers that will most likely terminate their relationship as a result of the breach incident." PONEMON INSTITUTE, LLC, 2007 ANNUAL STUDY, *supra* note 71, at 7.
[199] Jennifer McAdams, *After the Data Breach: Navigating State Disclosure Laws*, COMPUTERWORLD, Oct. 29, 2007.
[200] PONEMON INSTITUTE, LLC, 2007 ANNUAL STUDY, *supra* note 71, at 7.
[201] PRNEWSWIRE, *supra* note 60.
[202] Claburn, *The Costs of Data Loss Rises*, *supra* note 59.
[203] *Id.*
[204] *Id.*

[47] In addition to loss of goodwill are the costs associated with "reputation management and customer support costs including information hotlines and credit monitoring subscription for victims."[205] Victims of privacy theft suffer adverse effects on insurance and credit rates, difficulty in obtaining credit, as well as struggles in seeking employment.[206] Clearly, if the consumer is bearing the burden of a company's malfeasance, it is unlikely that they will remain a loyal customer. The adverse effects of customer turnover can cause unforeseeable and lasting reductions in revenue.[207]

VIII. THE WRITING ON THE WALL

[48] As the preceding demonstrates, the responsible use of PII translates into substantial operational benefits and profit potential, while the failure to maintain and use PII properly creates enormous liabilities. PII directly affects a company's bottom line—whether it does so positively or negatively is largely the result of the manner in which the company approaches PII security. It is clear, therefore, that the leaders of corporate America must acknowledge the real value of PII by proactively protecting against the threats posed to PII and respecting an individual's privacy interest in such information.[208]

[49] The exact manner in which individual companies approach PII will, of course, depend upon the specific needs and capabilities of each company.[209] One necessary component, however, is increased involvement from corporate directors and officers.[210] Increased board involvement in protecting customer information has been advocated on numerous fronts. Federal banking agencies have promulgated guidelines

[205] *Id.*
[206] IDENTITY THEFT RESOURCE CENTER, *supra* note 192, at 4, 13.
[207] *See* PONEMON INSTITUTE, LLC, 2007 ANNUAL STUDY, *supra* note 71, at 3.
[208] *See* Foley, *supra* note 12, at 19 ("The risks and threats from inadequate information technology and data security are real and significant. They go to the heart of the company's existence and success and therefore demand careful attention from the board of directors and senior management.").
[209] This article does not endeavor to provide broad based protection plans, but rather seeks to reinforce the magnitude of the PII issue and, concomitantly, the fact that the issue requires the attention and action of directors and executives.
[210] Foley, *supra* note 12, at 19 ("Boards need to focus on information technology matters more frequently and in greater depth than in the past.").

that require directors to take an active role in protecting consumer information in the context of GLBA.[211] Although these guidelines are directed to the financial sector, the basic principles are applicable across many industries. In addition to the banking agencies, courts have acknowledged the role of directors in information security.[212] Similar direction is emanating in the private sphere from business groups including the Business Roundtable and the Corporate Governance Task Force,[213] as well as private practice attorneys.[214]

[50] The writing is on the wall: corporate protection of an individual's PII creates revenue growth opportunities and the failure to do so creates financial liabilities. Whether the directors and executives steering corporate America heed the growing calls to actively ensure that their companies protect PII will have a significant impact on not only the future of U.S. commerce, but also on the privacy of each citizen that takes part in electronic commerce. This includes the directors and executives themselves, who are, after all, active participants in commerce. The long corporate history of appropriate technological protection of financial assets provides corporations with a roadmap for the comparable treatment of PII. Hopefully, America's corporate leaders will read the writing on the wall and apply the knowledge and experience they have attained protecting financial assets to the protection of PII before it is too late, for commerce and for privacy.

[211] Specifically, the guidelines direct boards of directors, or appropriate committees to "(1) [a]pprove the bank's written information security program; and (2) [o]versee the development, implementation, and maintenance of the bank's information security program, including assigning specific responsibility for its implementation and reviewing reports from management." 12 C.F.R. pt. 30, app. B.III.A.

[212] *See* Taft, *supra* note 13, at 501-02 (discussing *In re* Caremark Int'l Inc. Derivative Litig., 698 A.2d 959 (Del. Ch. 1996)).

[213] *Id.* (discussing *In re* Caremark Int'l Inc. Derivative Litig., 698 A.2d 959 (Del. Ch. 1996)).

[214] *See* Foley, *supra* note 12, at 17 ("As the opportunities and risks arising out of the use of information technology in modern business have expanded, so has the need for board of directors' oversight."). Mr. Foley suggests a "combination of oversight by a specialized technology committee and limited oversight by [an] audit committee." *Id.* at 19.