Protecting Information Security Under a Uniform Data Breach Notification Law

Kathryn E. Picanso

Follow this and additional works at: https://ir.lawnet.fordham.edu/flr

Part of the Law Commons

Recommended Citation
Available at: https://ir.lawnet.fordham.edu/flr/vol75/iss1/9

This Article is brought to you for free and open access by FLASH: The Fordham Law Archive of Scholarship and History. It has been accepted for inclusion in Fordham Law Review by an authorized editor of FLASH: The Fordham Law Archive of Scholarship and History. For more information, please contact tmelnick@law.fordham.edu.
Protecting Information Security Under a Uniform Data Breach Notification Law

Cover Page Footnote
J.D. Candidate, May 2007, Fordham University School of Law. I would like to thank Professor Joel Reidenberg and JoAnn Kamuf their advice, guidance, and editing suggestions.
PROTECTING INFORMATION SECURITY UNDER A UNIFORM DATA BREACH NOTIFICATION LAW

Kathryn E. Picanso*

INTRODUCTION

In 2004, a major retailer announced that unauthorized access to its in-store computer systems exposed thousands of customer credit card accounts to potential misuse.¹ Unbeknownst to the retailer, the vendor who implemented the credit card processing software had configured the software to improperly retain unencrypted customer credit card information in its log files.² The retailer was unaware of the problem until informed by credit card issuing banks, which noticed fraudulent purchases totaling several million dollars made using counterfeit copies of their customers' credit and debit cards.³ These issuing banks had to cancel and reissue thousands of cards and later sought to recoup their costs.⁴ Subsequent litigation involved the retailer, software vendor, merchant bank, and credit card issuing banks, leading to millions of dollars in potential liability for the defendants and ensuring further publicity concerning the security breach.⁵ A regulatory investigation also ensued, followed by an enforcement action, which was later settled.⁶

---

* J.D. Candidate, May 2007, Fordham University School of Law. I would like to thank Professor Joel Reidenberg and JoAnn Kamuf their advice, guidance, and editing suggestions.


4. See id.

5. See infra Part II; see also BJ's Wholesale Club, Quarterly Report (Form 10-Q), at 9 (Oct. 29, 2005), available at http://www.sec.gov/Archives/edgar/data/1037461/000119312505229785/d10q.htm (noting that the amount of outstanding claims against the corporation resulting from the breach—approximately thirteen million dollars—was primarily from credit card issuing banks).

6. See Bank, supra note 2.
Similar scenarios have played out in the news in recent years. A disclosure of security breaches, many spurred by state legislation, has highlighted the need for better protection of information systems. In 2005 alone, Citifinancial, Bank of America, Choicepoint, DSW, Ameritrade, CardSystems, LexisNexis, Time Warner, and over forty colleges and universities reported security breachers involving the loss or theft of personal information.

The number of people potentially affected appears considerable. Citigroup lost computer tapes containing sensitive data on 3.9 million accounts as they were shipped via UPS from New Jersey to Texas. Bank of America lost data on as many as 1.2 million credit card customers. A security breach by hackers at CardSystems Solutions, which processes credit card transactions and other payments for banks and merchants, left nearly forty million Visa and MasterCard accounts compromised. Consumer data aggregator Choicepoint provided personal information on approximately 145,000 individuals to criminals posing as legitimate businesses.

Litigation and enforcement actions arising from these breaches are growing as well. Lawsuits seeking class action status are proceeding in California against CardSystems, MasterCard International, Visa USA, and Choicepoint for the security breaches described above. The Federal Trade Commission (FTC), as well as states' attorneys general, has launched investigations into a number of companies, including both Choicepoint and CardSystems, for unfair practices.

This Note examines state and federal responses to information security issues and suggests a proper framework for legislation in this area. Part I of this Note discusses the problems posed by poor information security, describes current federal and state efforts to force businesses to secure their information networks and disclose any breaches resulting in potential exposure of personal data, and comments on the relationship between state

14. See McTaggart & Eleftheriou, supra note 12; Shawna McAlearney, BJ’s Settlement with FTC Bodes Ill for Others, SearchSecurity.com, June 20, 2005, http://searchsecurity.techtarget.com/originalContent/0,289142,sid14_gci1099579,00.html.
and federal laws. Part II considers potential judicial and statutory approaches to protecting data security at the federal and state level. This part examines state litigation and analyzes some of the issues confronting plaintiffs who seek to recover damages under a negligence theory. Federal proposals for a uniform data security and breach law are also considered, along with their potential impact on current state models. Finally, Part III concludes with a recommendation for a regulatory framework that addresses the concerns for uniform data security regulations while maintaining the consumer protections guaranteed under state legislation.

I. THE NEED FOR STRONGER INFORMATION SECURITY CONTROLS

Information is increasingly being gathered, used, and distributed in electronic form.15 Networked information systems that facilitate the exchange of electronic information between computer devices have become indispensable to businesses, governments, and individuals, but this reliance has come with increased vulnerabilities.16 As networked computer systems have grown in importance and use, the need for better information security measures to protect these systems has also grown. Securing the data stored, processed, transmitted, and received by networked information systems is therefore critical.17 Attacks targeting network vulnerabilities can come from external sources—such as viruses,18 worms,19 and denial of service attacks20—or from internal sources—such as careless or even disgruntled employees.21 When information systems house highly confidential data, or

---


18. A virus is a computer program that replicates by gaining access to a computer and inserting copies of itself into computer files. See Aaron Schwabach, Internet and the Law: Technology, Society, and Compromises 303 (2006). Computers infected with viruses may experience no harm, may slow down or crash, or may have their files corrupted or deleted. See id.

19. Often confused with viruses, worms gain “backdoor” access to computers and frequently install programs without users’ knowledge. See id. at 318-20.

20. Infected computers can serve as “zombies” and launch denial-of-service attacks, in which a large number of requests for access to a Web site, usually generated by “captured” computers, renders the site unable to respond to requests by regular users. See id. at 83-84.

21. See D. Reed Freeman, Jr., Nat’l Legal Ctr. for the Pub. Interest, Information Security for In-House Counsel: Reducing the Risk of Liability from Hacks, Attacks, and Other
perform critical functions, the results of attacks and security breaches can be disastrous.

Poor information security presents a number of problems. Most directly, insecure networks are susceptible to security attacks. In a survey conducted by the Computer Security Institute and the FBI’s Computer Intrusion Squad, nearly sixty percent of respondents detected computer security breaches in 2005. The consequences of the attacks can vary from network downtime or delays, to compromised or damaged records and files, to no discernable impact at all.

Network attacks can have serious ramifications on national security, as both the military and the national economy are increasingly reliant on critical infrastructures and information systems. Critical infrastructures are “those physical and cyber-based systems essential to the minimum operations of the economy and government,” many of which are privately owned and operated. Recognizing that the failure to protect information networks could disrupt essential operations, and cause loss of revenue, intellectual property, and even life, the federal government has called for collaboration between industry, government, academia, and nongovernmental groups to protect the nation’s critical infrastructure, but has stopped short of imposing specific security measures.

Identity theft, the fraudulent use of another person’s personal information, usually for economic gain, is another potential consequence of inadequate security controls. This type of fraud generally involves the misuse of existing credit card, checking, savings, and phone accounts, or the misuse of personal information for various uses, such as opening new accounts and taking out new loans, renting an apartment, or receiving...

23. Id.
PROTECTING INFORMATION SECURITY

medical care. A 2003 FTC survey revealed that nearly ten million consumers discovered they were victims of some sort of identity theft in the preceding twelve months. The consequences are costly in terms of time and money: In 2003 alone, the cost of identity theft was estimated at forty-eight billion dollars, and the average victim spent thirty hours correcting records and clearing their reputation, often with no ability to recover damages.

Beyond the direct cost of damages to businesses, poor information security can lead to declining consumer confidence in electronic and Internet transactions and lost customers. Recent surveys suggest that this may already be happening, even though the problem of electronic identity theft may be less pronounced than consumers realize. While the cost estimates of security breaches vary due to different methodologies for calculating costs, overall damages to businesses can be substantial. In addition to the costs of remedying problems arising from security breaches—such as replacing credit cards and providing free credit monitoring—businesses can also suffer from dips in stock prices, damage to reputation, and potential civil and even criminal liabilities.

29. See id.
31. See id. at 7.
32. See Dinesh C. Sharma, Data Leaks Denting Web Shoppers’ Confidence, CNet News.com, June 23, 2005, http://news.com.com/Data+leaks+denting+Web+shoppers+confidence/2100-1029_3-5759294.html (citing two recent studies by the market researcher Gartner, and the nonprofit research group, The Conference Board, which show, respectively, that 75% of online shoppers are more cautious about where they buy goods online, and over 50% of internet users say their level of concern has grown); see also Ponemon Inst., National Survey on Data Security Breach Notification (2005), http://www.whitecase.com/files/FileControl/863d572d-cde3-4e33-903c-37eaba537060/7483b893-e478-44a4-8fed-f49aa917d8cf/Presentation/File/Security_Breach_Survey%5b1%5d.pdf (reporting the results of a survey sponsored by the law firm White & Case LLP and conducted by the Ponemon Institute LLC, which found that after being notified of a breach, nearly 20% of respondents said they ended a relationship with a company, 40% said they were thinking about ending their relationship, and 5% said they hired a lawyer).
35. See Paul D. Shaw, Managing Legal and Security Risks in Computing and Communications 2 (1998) (noting possible consequences of litigation arising from breaches, such as costs, harm to reputation, and harm to customer and investor relations); Smedinghoff, supra note 13, at 12; see also Gregg Keizer, Report: Security Slip-Ups Don't Ding Stock Prices for Long, TechWeb News, Sept. 23, 2005, http://www.techweb.com/wire/security/171200329 (discussing a research paper that noted stock price decreases for companies, like Choicepoint and Cardsystems, whose core business
A. The Role of Knowledge Sharing in Risk Assessment

Information sharing and disclosure improves security by helping to identify vulnerabilities, establish best practices, raise better defenses, and mitigate attacks.36 One of the initial steps in most information security programs is a risk assessment to identify and understand threats to the confidentiality, integrity, and availability of information and information systems, followed by a determination of the appropriate levels of training, controls, and testing necessary to mitigate those risks.37 Throughout this process, alternative strategies for dealing with risk are considered and decisions are made as to the level of risk acceptable to an organization.38 Understanding the acceptable level of risk allows management to make well-informed decisions to justify information security expenditures.39

More data on attacks, intrusions, and security breaches is essential to improving overall information infrastructure protection.40 Models used to assess risk require information on the actual numbers of events, the costs of those events, and the cost of implementing security controls, but the total number of security breaches and breach attempts is uncertain.41 Undoubtedly a large number of breaches and attempts go undetected, and was affected by security breaches, but only temporary harm to the stock prices of other businesses).

36. See Comm. on Critical Info. Infrastructure Prot. and the Law, Nat'l Res. Council, Critical Information Infrastructure Protection and the Law: An Overview of Key Issues 17 (Stewart D. Personick & Cynthia A. Patterson eds., 2003) [hereinafter Critical Information Infrastructure Protection] (analyzing the legal issues involved in information security). Examples of industry suggestions to most effectively improve security issues include the sharing of information about potential threats and best practices for protecting against such threats, and establishing a single point of contact for administrators of backbone ISPs to share real-time information about attacks. Id.


38. See Soo Hoo, supra note 34, at 3, 12 (arguing that the information security insurance needs, liability exposure, and market competition will help shape a new quantitative framework for managing risk).


40. See Frye, supra note 16, at 370 (arguing for governmentally mandated full reporting of cyberintrusions and measurable damages to overcome market incentives preventing disclosure of information); see also Critical Information Infrastructure Protection, supra note 36, at 17.

41. See Soo Hoo, supra note 34, at 4, 29 (discussing the Annual Loss Expectancy Model ("ALE"), a common metric used in risk-management modeling first proposed by the National Bureau of Standards in 1979).

42. See id.

43. See id. at 30 (citing a Defense Information Systems Agency 1996 report estimating that 96% of successful break-ins were undetected, and only 27% of detected break-ins were reported).
of the ones that are detected, only a subset get reported because businesses are wary of revealing security breaches and breach attempts.\footnote{See Critical Information Structure Protection, \textit{supra} note 36, at 18-19; see also CSI/FBI Survey, \textit{supra} note 22, at 18-19 (reporting that while 63\% of respondents reported sharing information regarding computer intrusions, only 20\% reported intrusions to law enforcement).}

This hesitation on the part of businesses to report security intrusions stems from a number of factors, including fears of increased liability, antitrust litigation, loss of proprietary information, and harm from negative publicity.\footnote{See Frye, \textit{supra} note 16, at 374-76; see also Critical Information Infrastructure Protection, \textit{supra} note 36, at 24-33. Antitrust law seeks to discourage collusion among companies and increase competition in the marketplace. For this reason, companies fear that information sharing may be viewed as collusive and therefore anticompetitive. See Critical Information Infrastructure Protection, \textit{supra} note 36, at 30.} Recognizing the need for such collaboration and disclosure, the federal government has sought to allay these fears and encourage information sharing in the private sector.\footnote{See supra notes 24, 39.} Presidential directive PD-63, issued by President Clinton in 1998, called for the creation of industry-specific Information Sharing and Analysis Centers ("ISACs") to encourage industries to gather, analyze, and disseminate information when appropriate.\footnote{See Presidential Directive 63, \textit{supra} note 25.} ISACs have been created in several industries, including the financial services, information technology, electric power, telecommunications, chemical and rail industries.\footnote{See \textit{Dep’t of Homeland Sec., Threats and Protection: Information Sharing \\& Analysis Centers}, \url{http://www.dhs.gov/dhspublic/display?theme=73&content=1375} (last visited Aug. 20, 2006).} Government attempts to promote information sharing and business collaboration have had mixed success, however, and currently most information sharing occurs through informal channels.\footnote{See Critical Information Infrastructure Protection, \textit{supra} note 36, at 18 (noting that most ISACs are still in their infancy or planning stages); CSI/FBI Survey, \textit{supra} note 22, at 20 tbl.23. Survey results show that 46\% of respondent organizations do not belong to any information sharing organization, although that percentage may be lower among organizations in general. The authors of this study acknowledge that the respondents may be more "security savvy" than general information technology professionals because they are all members or conference attendees of the Computer Security Institute and have shown a heightened interest in information security. CSI/FBI Survey, \textit{supra} note 22, at 5.} Much of the legislation in the area of information security, as described in Part II, seeks to deal with these problems of nondisclosure.

Despite the potential risks associated with lax security procedures, not all businesses take necessary precautions against security lapses.\footnote{See Scott Berinato, \textit{Six Secrets of Highly Secure Organizations}, \textit{CIO} Magazine, Sept. 15, 2004, at 51, \url{available at http://www.cio.com/archive/091504/security.html} (reporting that of the thirty security priorities named in the 2003 survey, many respondents fell short on implementing twenty-eight of those measures).} In the absence of adequate self-regulation, federal and state governments have stepped in and required businesses to protect their information assets. The
following section discusses some of the obligations arising from federal and state legislation.

B. Current Information Security Obligations

Corporate computer security is governed by a patchwork of state and federal statutes and regulations. While a number of those statutes impose criminal penalties for individuals who intentionally hack into network systems, this Note discusses laws imposing obligations on corporations to secure data and computer networks against attacks, intrusions, or system failures, and to disclose information to affected individuals regarding security breaches.

1. Obligations to Protect Information Systems and Data

At the federal level, governmental agencies responsible for promulgating regulations have taken a process-oriented approach to information security. Rather than mandate specific technical measures, these regulations require the implementation of a comprehensive security program suitable to an organization’s needs. Organizations covered by these regulations must assess the vulnerabilities of their information technology systems, estimate the likelihood that injurious scenarios may occur, and take appropriate steps to mitigate those risks. This approach was first seen in the Children’s Online Privacy Protection Act (COPPA) of 1998, but most of the development in this area has resulted from the enactment of the Gramm-Leach-Bliley Act (GLBA) and the implementation of the FTC’s Safeguards Rule.  

---


52. See Smedinghoff, supra note 13, at 13.


54. See Smedinghoff, supra note 13, at 13.


57. 16 C.F.R § 314.4.
The GLBA, also known as the Financial Services Modernization Act of 1999, laid out this process-oriented approach in security regulations for the financial industry. The purpose of the GLBA was to “modernize” the financial services industry by repealing regulations that prevented the merger of banking, insurance, and securities companies. To assuage fears that newly merged companies would have unrestricted access to an incredible amount of personal information, the Act set notification requirements on the use of personal information, mandating that a financial institution provide privacy notices to customers detailing what type of nonpublic personal information the institution collects, with whom the institution shares the information, and how it protects the information.

Under the GLBA’s privacy obligation policy, “each financial institution has an affirmative and continuing obligation to respect the privacy of its customers and to protect the security and confidentiality of those customers’ nonpublic personal information.” The Act requires financial corporations to (1) establish appropriate standards for administrative, technical, and physical safeguards that will ensure the security and confidentiality of customer information, (2) protect the security of these records against any anticipated threats, and (3) protect against unauthorized access or use of this information, which could result in substantial harm or inconvenience to customers.

Various federal agencies, including the FTC, are responsible for promulgating the information security procedures for the different sectors.


60. See generally Chris Jay Hoofnagle & Emily Honig, Victoria’s Secret and Financial Privacy, http://www.epic.org/privacy/glba/victoriassecret.html (last visited Aug. 20, 2006) (reporting on the role that a Victoria’s Secret catalog may have played in generating Congressional Republican support for the privacy provisions of the GLBA).

61. See FTC, In Brief: The Financial Privacy Requirements of the Gramm-Leach-Bliley Act, http://www.ftc.gov/bcp/conline/pubs/buspubs/glbshort.htm (last visited Aug. 20, 2006). The privacy notice should also provide information on how consumers and customers can choose to opt out of sharing arrangements between the financial institution and its affiliates, a right provided under the Fair Credit Reporting Act. Id.


of the financial industry (known as the "Interagency Guidelines"). These agencies are also charged with enforcing the regulations over the respective financial institutions subject to their jurisdiction. The FTC’s set of standards for the protection of customer records and information, known as the Safeguards Rule, has had the greatest impact through the FTC’s enforcement actions against financial and nonfinancial organizations. The FTC’s rule covers any financial institution that handles customer information, including not only institutions that collect nonpublic personal information from their own customers, but also those financial institutions that receive customer information from other financial institutions.

The Safeguards Rule requires financial institutions to “develop, implement, and maintain a comprehensive information security program that . . . contains administrative, technical, and physical safeguards that are appropriate to [the institution’s] size and complexity, the nature and scope of . . . activities, and the sensitivity of any customer information at issue.” The required administrative safeguards under the Rule include the following: designating someone to coordinate the information security program; performing a risk assessment that considers personnel training, information systems, and the detection, prevention, and response to attacks, intrusions, and other systems failures; designing and implementing safeguards to control risks and regularly testing safeguards to monitor effectiveness; overseeing service providers by ensuring that they are able to take appropriate security precautions and in fact do so; and updating the security program as necessary in response to frequent monitoring and material changes in the business.

A security breach need not occur for the FTC to take action: “[A]n actual breach of security is not a prerequisite for enforcement under Section 5 [of the Federal Trade Commission Act]; however, evidence of such a breach may indicate that the company’s existing policies and procedures were not adequate.” The commission acknowledges, however, that “perfect security” is not attainable, and breaches can occur even where every reasonable precaution has been taken.

64. See 15 U.S.C. § 6805(b). For examples of these standards, see supra note 52.
67. See 16 C.F.R. § 314.1(b).
68. Id. § 314.3(a).
69. See id. § 314.4.
71. See id.
Armed with the Safeguards Rule, the FTC has embarked on an aggressive strategy of investigations, enforcement actions, and settlements with companies that have agreed to implement the regulations and obtain independent security audits for a set period of time. Enforcement actions originally targeted mortgage companies for failure to comply with the basic requirements of the Rule, and also nonfinancial institutions whose privacy statements were found to have false and misleading information in light of subsequent security breaches. For example, Petco Animal Supplies, Inc., settled FTC charges that a security flaw in its Web site allowed hackers to access consumer records, including credit card numbers, in violation of privacy promises made to customers. The FTC alleged that Petco could have taken simple steps to prevent the type of attack that occurred and that credit card information would not have been accessed by intruders had the data actually been encrypted, as Petco claimed on its Web site. The FTC charged that these claims were deceptive and violated the Federal Trade Commission Act. “Consumers have the right to expect companies to keep their promises about the security of the confidential consumer information they collect,” said the Acting Director of the FTC’s Bureau of Consumer Protection. “The FTC will hold companies to their word.”

Recently, however, the FTC has expanded the reach of the Safeguards Rule beyond financial institutions and businesses with false and misleading privacy statements, to those nonfinancial institutions that experience security breaches due to lax information security policies and procedures. The FTC derives its authority over the information security practices of nonfinancial institutions from Section 5(a) of the Federal Trade Commission Act, which prohibits unfair and deceptive trade practices.

72. See In re Sunbelt Lending Services, Inc., No. C-4129, 2005 WL 120875 (FTC Jan. 3, 2005) (alleging that company failed to perform a risk assessment, implement reasonable policies and procedures, train employees, oversee the collection of customer information through its web site, and ensure that service providers were providing appropriate security); In re Nationwide Mortgage Group, Inc., No. 9319, 2004 WL 3142856 (FTC Nov. 9, 2004) (similar allegations). Both companies settled charges with the FTC and agreed to implement security procedures and submitted to biennial security audits by a third party professional for ten years. See In re Nationwide Mortgage Group, Inc., No. 9319, 2005 WL 996696 (FTC Apr. 12, 2005); In re Sunbelt Lending Services, Inc., 2005 WL 120875.


74. See id.

75. See id.

76. Id. (citing statements made by Lydia Parnes, Acting Director of the FTC’s Bureau of Consumer Protection).

77. Id.

78. See, e.g., In re DSW, Inc., No. 052-3096, 2005 WL 3366974 (FTC Dec. 1, 2005) (alleging that the failure to provide adequate security measures, which compromised over one million debit and credit cards, constituted an unfair act or practice); In re BJ’s Wholesale Club, Inc., No. C-4148, 2005 WL 2395788 (FTC Sept. 20, 2005) (alleging that maintaining a record of account information in violation of industry standards and failure to adopt adequate security measures was an unfair practice).

Under this general enforcement authority, the FTC can investigate and pursue actions against businesses whose activities qualify as practices that "cause or are likely to cause consumers substantial injury that is neither reasonably avoidable by consumers nor offset by countervailing benefits to consumers or competition."80

b. FTC Expansion of the Safeguards Rule

The first action expanding the scope of the FTC's authority beyond deceptive practices involved BJ's Wholesale Club, Inc., in a scenario similar to the one described in the introduction.81 In March of 2004, BJ's announced that unauthorized access to its computer systems from at least November 2003 to February 2004, resulted in the possible theft of personal information, including names and credit card numbers, from thousands of customers.82 BJ's did not notice the breach until informed that several million dollars of fraudulent purchases had been made with counterfeit copies of credit and debit cards by banks that had issued the credit cards to customers.83 In this enforcement action, the FTC pursued the broader strategy of alleging that the failure to ensure adequate security measures constituted an unfair practice.84 The Commission did not claim that BJ's made misrepresentations to their customers, as in the Petco action. Rather, it charged that BJ's failure to provide adequate security measures constituted an unfair practice that violated federal law.85 The agency contended that BJ's failed to encrypt personal data while in transit or when stored on the computer networks of their stores; created unnecessary risks by storing information longer than necessary in violation of bank rules; stored personal data in easily accessible files; failed to take adequate steps to prevent unauthorized wireless connections; and failed to take reasonable measures to detect unauthorized network access or conduct security audits.86

In a signed consent decree that did not acknowledge any wrongdoing, BJ's agreed to a settlement requiring the implementation of a comprehensive security program.87 The retailer promised to designate someone responsible for the information security program, perform a risk assessment, take "reasonable safeguards" to mitigate risks, test and monitor safeguards, and adjust the program in response to material changes—

80. Identity Theft Hearing, supra note 70, 5-6 (citing 15 U.S.C. § 45(n)).
81. See supra notes 1-5 and accompanying text.
83. See id.
84. See id.
85. See supra note 6 and accompanying text.
86. See id.
87. See id.
essentially the requirements of the FTC's Safeguards rule. BJ's also agreed to perform biennial security audits for the next twenty years.

c. State Consumer Fraud Statutes

State attorneys general have also pursued enforcement actions against companies engaging in improper data security practices under consumer fraud statutes. In general, these statutes prohibit all deceptive practices and misrepresentations, whether intentional or not, and are used to encourage better compliance with accepted security standards. Many states allow both attorneys general and injured private parties to bring suit, and at least two allow class action suits.

The enforcement actions pursued under these statutes are similar to the FTC's actions, as one example, involving the magazine publisher Ziff-Davis, shows. The company reached a settlement agreement with the attorneys general of Vermont, New York, and California, in which it agreed to implement better security procedures after it had inadvertently placed the personal information, including credit card numbers, of some of its subscribers on its Web site. Statements made by the company that it used "reasonable precautions" to keep consumer information secure, when it had not implemented adequate security measures, were considered false statements under the states' respective consumer fraud statutes.

The terms of the settlement required Ziff Davis to identify data security vulnerabilities; implement a risk assessment plan which included employee training, response procedures, and monitoring of information systems; encrypt data; control access to consumer data; and assess applications for security risks before any implementation. The company also agreed to...

88. See supra note 3 and accompanying text.
89. See id.
90. See, e.g., In re Eli Lilly, Inc., Assurance of Voluntary Compliance and Discontinuance, available at http://www.epic.org/privacy/medical/lillyagreement.pdf. Eli Lilly sent an e-mail to subscribers of their Prozac.com site, and accidentally disclosed all other subscribers' e-mails in the "To" field. id. ¶¶ 1.2-1.4, 2.4-2.5. In addition to implementing reasonable security procedures, the company paid $160,000 to the eight states pursuing the action. id. ¶¶ 5.4, 5.8.
94. See id. at 3-4. The respective statutes violated were Cal. Bus. & Prof. Code §§ 17200, 17500 (prohibiting unlawful, unfair or fraudulent business practices and untrue or misleading advertising); N.Y. Exec. Law § 63(12) (McKinney 2002) (prohibiting repeated, fraudulent, and/or illegal business activities); N.Y. Gen. Bus. Law §§ 349-350 (allowing the New York Attorney General or any injured person to bring suit against anyone committing "[d]eceptive acts or practices in the conduct of any business, trade or commerce"); Vt. Stat. Ann. tit. 9, § 2451 (prohibiting deceptive business practices and false advertising). In re Ziff Davis Media, supra note 93, at 4.
95. See In re Ziff Davis Media Inc., Assurance of Discontinuance, supra note 93, at 5-6.
pay $100,000 divided among the three states, and $500 to each consumer who submitted credit card information.96

While enforcement actions by the FTC and states' attorneys general may motivate businesses to better protect data against security breaches and raise awareness of security issues, most of the recent attention regarding data security has come from the large numbers of security breach disclosures reported under state notification laws.97

2. The Obligation to Disclose Information

Recognizing the injurious effect that security breaches can have on individuals and corporations, both the federal government and state legislatures have passed measures requiring the disclosure of information related to security breaches, and more legislation may be forthcoming.98

a. State Regulations

The most prominent breach notification legislation is California's Database Breach Notification Security Act ("SB 1386"), enacted in 2002.99 The statute requires any organization doing business in California to disclose to "resident[s] of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person."100 The purpose of SB 1386 is to help consumers protect themselves against identity theft, or minimize the damage if a crime has already occurred, by informing consumers expeditiously of possible misuse of their personal information.101 To that end, SB 1386 provides a private right of action for any person harmed by a failure of a business or organization to give notice.102

Since the law was enacted, over ninety organizations have reported security breaches that have resulted in the exposure, theft, or loss of almost

96. See id. at 7-8.
97. See Privacy Rights Clearinghouse, supra note 8.
98. See infra Part II.A.
100. Cal. Civ. Code § 1798.82(a) (West Supp. 2005). Personal information includes name in combination with social security number, driver's license number, state identification card number, and any account number that would allow access to an individual's financial account. Id.
101. See id. (historical and statutory notes). Notice is to be given in the "most expedient time possible and without unreasonable delay," unless a law enforcement agency believes that notification will interfere with a criminal investigation. Id. § 1798.82(a), (c).
ninety million records. Widespread publicity over these disclosures has led to the enactment of similar laws in over twenty states, and the introduction of a number of Congressional House and Senate bills with similar security breach disclosure requirements. While hailed by privacy and consumer advocates as a much-needed tool against lax security practices, a number of issues still remain, such as when notice must be provided.

b. Federal Regulations

Existing federal regulations impose reporting requirements on certain businesses. Under the GLBA regulations, financial institutions should implement a "risk-based response program to address incidents of unauthorized access to customer information in customer information systems." At a minimum, institutions should determine the scope of the breach, take steps to control further unauthorized access or use of customer information, notify the appropriate federal regulating agency and law enforcement authorities, and inform customers if the institution believes that their information has been, or could reasonably be, misused.

A company may find itself subject to both GLBA's and state statutory requirements in the event of a breach. Only to the extent that such statute is inconsistent with the specified provisions of the Act will the GLBA supersede state statutes or regulations. The GLBA does not preempt more protective state laws and includes a savings clause, which provides that "a State statute, regulation, order, or interpretation is not inconsistent...if the protection such statute, regulation, order, or interpretation affords any person is greater than the protection provided...as determined by the [FTC]." Given the overlapping nature of much federal legislation, however, this clause has not prevented preemption of

103. See Privacy Rights Clearinghouse, supra note 8.
106. See Skinner, supra note 102, at 21-26 (noting that the complexity of online transactions makes the scope of the notice provision difficult to determine).
108. See id. II.A., III.A.
110. Id. § 6807(b).
state privacy statutes by other statutes, and federal preemption of state laws remains a concern of many consumer advocates.111

c. Federal Preemption of State Protections

Calls for federal legislation mandating adequate security measures for sensitive data are tempered by concerns that such legislation may water down existing state protections.112 Acts of Congress can preempt state legislation and judicial precedents under both express and implied preemption principles.113 Express preemption requires a determination of whether a state statute or requirement falls within the scope of a stated preemption provision.114 Implied preemption, requiring a determination of congressional intent, can occur under two circumstances.115 The first involves instances where a regulatory scheme is so pervasive that it is reasonable to conclude the Congress intended to occupy an entire field.116 This type of preemption, seen in areas like management-labor relations,117 medical devices,118 and oil tankers,119 requires a “clear and manifest purpose” that Congress intended to occupy the field.120

---

111. In Bank of Am., N.A. v. City of Daly City, Cal., 279 F. Supp. 2d 1118, 1126 (N.D. Cal. 2003), vacated, Bank of Am. v. Alameda County, 2004 U.S. App Lexis 14582 (9th Cir. 2004), the court held that the GLBA’s saving clause did not prevent provisions of a local consumer privacy notice prohibiting financial institutions from sharing information to their affiliates from being preempted by the Fair Credit Reporting Act. The case was later vacated on appeal, presumably because the local ordinance in question was repealed. See Anne P. Fortney, Uniform National Standards for a Nationwide Industry: FCRA Preemption of State Laws Under the Fact Act, 58 Consumer Fin. L.Q. Rep. 259 (2004).

112. See Ctr. for Democracy & Tech., supra note 105 (warning that the Center would oppose any legislation that weakened existing state laws); see also Brian Krebs, States Keep Watchful Eye on Personal-Data Firms, washingtonpost.com, June 1, 2005, http://www.washingtonpost.com/wp-dyn/content/article/2005/06/01/AR2005060100359_pf. html (quoting Montana Attorney General, Mike McGrath, who said that states would fight vigorously to oppose federal legislation that would supersede state laws).


114. See generally CSX Transp., Inc. v. Eastwood, 507 U.S. 658, 664 (1993) (“If the statute contains an express pre-emption clause, the task of statutory construction must in the first instance focus on the plain wording of the clause, which necessarily contains the best evidence of Congress’ pre-emptive intent.”).


117. See, e.g., Garner v. Teamsters Union, 346 U.S. 485 (1953) (finding that state courts may not grant injunctions against activities prohibited by the National Labor Relations Board).

The second circumstance occurs when there is an actual conflict between the federal and state legislation, either because the state law stands as an obstacle to the accomplishment and execution of the full purposes and objectives of Congress, or because compliance with both state and federal laws is impossible. "Obstacle preemption," as this latter type has become known, has been criticized as a default doctrine in situations where Congress’s intent to preempt cannot be determined, or where there is not a significant need for national uniformity in the particular field. There is often said to be a presumption against preemption, although it is unclear whether this applies generally, or operates only in fields traditionally occupied by the states, like health and safety.

Recent decisions suggest that federal preemption remains a possibility, even with a savings clause similar to the one seen in the GLBA. In Geier v. American Honda Motor Co., the Court noted that neither an express preemption clause, nor a savings clause, "bar[s] the ordinary working of conflict preemption principles." In other words, courts will still consider whether a preemption clause supersedes a statute, and if it does not, courts must consider whether ordinary ("implied") preemption principles apply. If so, courts must then perform implied preemption analysis and determine whether a statute conflicts with federal legislation under actual or obstacle common law negligence claims against the manufacturer of an allegedly defective pacemaker.


120. Rice v. Santa Fe Elevator Corp., 331 U.S. 218, 230 (1947) (citing field preemption as one of the ways in which Congress evinces a clear and manifest purpose to supersede the historic police powers of the states).

121. See Hines v. Davidowitz, 312 U.S. 52 (1941) (ruling that state law which required aliens to register and carry an alien identification card was preempted by federal registration requirements).

122. See, e.g., Florida Lime & Avocado Growers, Inc. v. Paul, 373 U.S. 132, 142 (1963) ("The test of whether both federal and state regulations may operate, or the state regulation must give way, is whether both regulations can be enforced without impairing the federal superintendence of the field, not whether they are aimed at similar or different objectives.").


124. See Santa Fe Elevator Corp., 331 U.S. at 230 ("We start with the assumption that the historic police powers of the States were not to be superseded by the Federal Act unless that was the clear and manifest purpose of Congress.").

125. See, e.g., United States v. Locke, 529 U.S. 89, 108 (2000) ("[A]n assumption of nonpre-emption is not triggered when the state regulates in an area where there has been a significant federal presence.").

126. Geier v. Am. Honda Motor Co., 529 U.S. 861, 861, 869 (2000) (ruling that the a standard promulgated by the Department of Transportation (DOT) under the authority of the National Traffic and Motor Vehicle Safety Act preempted a negligence suit against the respondent car company for the failure to include a driver side air bag).

127. See id. at 867.
This same three-step analysis also applies to state tort lawsuits.\textsuperscript{128} In \textit{Sprietsma v. Mercury Marine}, involving a common-law tort suit against a boat manufacturer for failure to install propeller guards after the Coast Guard had specifically decided not to require such devices under the Federal Safety Boat Act (FSBA), the Court performed a similar analysis as in \textit{Geier}.\textsuperscript{130} It first focused on the wording of the preemption clause of the FSBA to determine congressional intent, concluding that the wording, along with the presence of a savings clause, permitted a narrow reading of the provision that excluded common law actions.\textsuperscript{131} It then performed an implied preemption analysis, finding no intent by Congress to occupy the field of boating safety, and no conflict between state common law suits and the “accomplishment and execution of the full purposes and objectives of Congress.”\textsuperscript{132}

The Court declined to find that a decision to forego regulation in a particular area, like the one made by the Coast Guard here, had “as much preemptive force as a decision to regulate,” though noting that it had the ability to make such a conclusion.\textsuperscript{133} Of particular importance seemed to be the position taken by the Coast Guard, the federal agency in question.\textsuperscript{134}

Federal preemption doctrine, especially preemption of state tort claims, remains unsettled.\textsuperscript{135} Any federal legislation involving data security measures will certainly impact state laws and regulations, and possibly state common law actions for damages. As will be seen in Part II.C.3, proposed federal bills deal with the issue of state law preemption in different ways.\textsuperscript{136}

\textsuperscript{128} See \textit{id.} The Court found that the preemption clause and savings clause excluded common-law actions, but held that the suit presented an obstacle to the DOT’s objectives of promoting safety by allowing a mix of passive restraint devices. \textit{Id.} at 868, 881.

\textsuperscript{129} See \textit{id.} at 867 (describing how a majority of the Court in \textit{Medtronic}, consisting of the plurality opinion and two concurrences, found that state common-law claims could be treated similarly to legislative “enactments”).


\textsuperscript{131} See \textit{id.}

\textsuperscript{132} \textit{Id.} at 66 (internal quotations omitted).


\textsuperscript{134} See \textit{id.} at 67-68. The Coast Guard had not imposed propeller guard requirements, in contrast to the DOT’s affirmative decision in \textit{Geier} to promote alternative protection systems, and it did not believe, as the DOT did, that a tort suit would stand as an obstacle to the execution of the objectives of the legislation in question. Moreover, it did not exhibit a concern that common-law suits would impede uniformity of manufacturing regulations across the industry.


\textsuperscript{136} See infra Part II.C for a discussion of proposed legislation.
3. Effectiveness of Current Regulations

The effectiveness of federal and state government regulations at improving corporate information security is unknown. While some indications point to stronger security procedures as more businesses seek to comply with regulations, other indications suggest that compliance percentages are still low. The latter also suggests that some signs of improvement may be mere window dressing.

Possible reasons for noncompliance with regulations may be that the patchwork of state and federal regulations is too confusing and difficult to comply with, that there are just too many regulations, or that businesses do not fear serious consequences for noncompliance, because the regulations are too vague, or governmental agencies are not devoting enough resources to enforcing them. Fears of litigation could actually play a stronger role in motivating businesses to dedicate more resources to information security than compliance with governmental regulations, which suggests that imposing liability on businesses may also help improve overall information security.

Whatever the reason for possible noncompliance, many authorities believe that more needs to be done, and advocate either streamlining current legislative requirements, or increasing the protections afforded to third parties.

---

137. Compare Ernst & Young, Global Information Security Survey 2005: Report on the Widening Gap (2005), available at http://www.ey.com/global/download.nsf/International/Global_Information_Security_Survey_2005/$file/EY_Global_Information_Security_survey_2005.pdf (reporting results from a survey of over 1,300 organizations which showed that compliance with regulations is the primary driver of information security), with Berinato, supra note 50 (reporting results from the “2004 Global Information Security Survey” which found that negative factors, such as the fear of litigation, remained primary drivers of security spending). Thirty-nine percent of organizations in the “2004 Global Information Security Survey” reported that government efforts to improve information security did not influence their security practices. See Compliance? What’s That?, CSO Magazine, Oct. 2005, at 28, available at http://www.csoonline.com/read/100105/survey-compliance.html (also reporting on results from the “2004 Global Information Security Survey”). According to the survey, 15% of respondents who needed to be in compliance with SB 1386 were not; 17% of respondents who needed to be in compliance with GLBA were not; 38% of respondents who needed to be in compliance with HIPAA were not; and 38% of respondents who needed to be in compliance with Sarbanes-Oxley were not. Id.

138. See Berinato, supra note 50 (noting that although security governance has improved as more businesses created a Chief Security Office (CSO) or Chief Information Security Officer (CISO) position (from 15% in 2003 to 31% in 2004), and implemented centralized security management systems (from 11% in 2003 to 39% in 2004), many information executives report their positions as lacking budget, staff, or authority); see also Ernst & Young, supra note 137 (noting that nearly 90% of respondents who are implementing security measures to comply with internal control regulations focus on creating and updating policies and procedures, while only 41% report that they are taking this opportunity to reorganize their information security function or change their security architecture).

139. See Compliance? What’s That?, supra note 137.

140. See Berinato, supra note 137 and accompanying text; Compliance? What’s That?, supra note 137 and accompanying text.
Part II of this Note looks at federal and state approaches to improving information security, through both legislative means and the court system.

II. APPROACHES TO IMPROVE INFORMATION SECURITY

The causes of noncompliance to date are not clear, nor is the course of action that will help alleviate security breaches. This section considers further regulatory proposals for protecting third parties from lax information security practices at both the federal and state level, focusing on security regulations and breach notification laws. This part also considers a possible common law framework of liability for security breaches and discusses current obstacles to such a framework. While stronger regulations and common law liability are not mutually exclusive options and can serve to complement one another, there are opposing views on whether civil liability should be imposed for companies whose lax information security results in data breaches.\(^\text{141}\)

The enactment of statutes and regulations, such as the GLBA, the FTC’s Safeguards Rules, and California’s Breach Notification Act, along with enforcement actions against businesses and disclosures of security breaches have been integral in raising awareness about the need for better information security.\(^\text{142}\) Part II.A considers existing federal responses to enhancing security measures, while Part II.B looks at state statutory and common law approaches targeting data security. Finally, Part II.C describes proposed federal legislation for a uniform breach notification law.

A. Federal Action to Enhance Security Measures

Many privacy advocates, commentators, and industry groups agree that Congress should extend the obligations imposed under the FTC’s Safeguards Rule to entities that store electronic data.\(^\text{144}\) Although the

\(^{141}\) See discussion infra Part II.

\(^{142}\) See Critical Information Infrastructure Protection, supra note 36, at 35 (noting that committee participants differed on whether the best way to promote critical infrastructure protection was to target hackers and other perpetrators or vendors and service providers, for negligent security policies and procedures).


\(^{144}\) See Identity Theft Hearing, supra note 70, at 10 (advocating for the extension of the FTC’s Safeguards Rule to organizations that are not financial institutions); Ctr. for Democracy & Tech., supra note 105 (similar); see also Oversight Hearing on Data Security, Data Breach Notices, Privacy and Identity Theft: Hearing Before the U.S. Senate Comm. on Banking, Housing, and Urban Affairs, 109th Cong. 3 (2005) (statement of Edmund Mierzwinski, Consumer Program Director, U.S. Public Interest Research Group) (calling for extending the “modest” protections to third-party processors, such as Card systems, and data brokers, such as Choicepoint), available at http://banking.senate.gov/files/ACFDC9B.pdf [hereinafter Data Security Hearing]; Examining the Financial Services Industry’s
Rule’s flexibility is often praised, some believe that the regulations do not go far enough and should be strengthened with more definitive standards for information security.145 Moreover, the FTC has been criticized for failing to enforce these rules and to aggressively pursue privacy protections.146

Inadequate enforcement of privacy and security protections has frequently been cited in calls for more rights that provide meaningful sanctions and redress. Advocates and commentators who recognize the importance of state-based approaches to privacy protection enforcement caution the federal legislature not to preempt the functions provided by state and local authorities.147 More specific recommendations for effective enforcement of security regulations include providing an express right of action, setting minimum liquidated damages provisions for companies that suffer security breaches due to negligence, and authorizing state attorneys general to fine companies and establish funds for victims.148

Recent bills considered in the U.S. House of Representatives and U.S. Senate during 2005 have varied with respect to the issue of improving data security, with some seeking to extend current regulations,149 and others seeming to undermine the protections.150 None of these bills provide a

145. See, e.g., Identity Theft Hearing, supra note 70, at 16-17 (statement of William H. Sorrell, Attorney General of the State of Vermont and President of the National Association of Attorneys General) (commenting that although the flexibility of the Safeguards Rule was initially appropriate, in light of recent security breaches, more definitive standards are needed); Editorial, Congress Must Deal with ID Theft, Wired, June 20, 2006, http://wired.com/news/privacy0,1848,67845,00.html (calling for stricter federal regulations, such as mandatory encryption of all sensitive data, development of simple rules specific to each industry, and funds for the FTC to enforce them).

146. See Protecting Consumer’s Data: Policy Issues Raised by Choicepoint: Hearing Before the House Subcomm. on Commerce, Trade, and Consumer, Protection, Comm. on Energy and Commerce, 109th Cong. 82 (2005) (statement of Marc Rotenberg, President, EPIC) (criticizing the FTC’s failure to investigate Choicepoint’s practices until it was too late).

147. See id.; Identity Theft Hearing, supra note 70, at 17 (statement of William H. Sorrell, noting the role of state attorneys general in investigations of security breaches).


149. See S. 1408, 109th Cong. § 2 (2005) (requiring any business entity or nonprofit organization that acquires, maintains, or utilizes sensitive personal information that acquires, maintains, or utilizes sensitive personal information to take similar precautions mandated under the GLBA); S. 1332, 109th Cong. § 402 (2005) (requiring more specific measures similar to the FTC’s Safeguards Rule, including the implementation of a comprehensive security program based on a risk assessment and ongoing risk management controls).

150. See H.R. 3997 Hearing, supra note 143 (statement of Evan Hendricks, Editor/Publisher, Privacy Times) (commenting on H.R. 3997, which mandates only “reasonable policies and procedures” and does not require a risk assessment or comprehensive security program).
private cause of action—enforcement is left either to the FTC, State Attorneys General, or the United States Attorney General.\footnote{151}

B. State Approaches to Enhancing Security Measures

At least two states, Arkansas and Nevada, have enacted legislation mandating reasonable security measures.\footnote{152} Neither bill offers substantial protection; both require entities that collect personal information to implement "reasonable" security procedures to protect against unauthorized access, destruction, use, modification, or disclosure of information.\footnote{153}

Even if states enact stronger legislation requiring businesses to protect their sensitive data, some proponents argue that businesses will not take adequate steps to secure sensitive data unless confronted with the threat of civil liability.\footnote{154} The next section considers liability for damages resulting from inadequate data security measures and obstacles to recovery.

1. Tort Liability

Some privacy advocates and security professionals believe that government regulations are not enough. Instead, they argue that applying common law rules to redress problems of negligent information security will motivate businesses to enact better policies and procedures and comply with industry standards in a more effective manner than a one-size-fits-all government regulation could.\footnote{155} Injured parties, whether individuals harmed by identity theft or corporations harmed by service providers, would have an avenue of redress. Tort liability could also help crystallize security standards, since many businesses seeking to minimize their liability would comply with industry-wide standards as a demonstration of due care.\footnote{156}

Cases involving damages from security breaches have been brought in court under various causes of action, such as negligence, breach of contract,
and breach of fiduciary duty. Courts have been reluctant, however, to allow recovery in many of these actions. While breach of contract actions remain the best basis on which to bring a claim, this doctrine is limited to instances where the plaintiff is in privity with the defendant. Due to the free-flowing nature of data and the growth of information brokers, like Choicepoint, injured parties frequently lack contractual relationships with the party responsible for protecting their personal information.

For these reasons, many advocates suggest that tort law may be the best way to protect personal data. Obstacles to imposing liability for security breaches still remain, however, including the initial determination as to whether such a duty exists, defining the standard of care, intervening acts of third parties breaking the chain of causation, and the economic loss doctrine. These hurdles are not insurmountable and may diminish as greater awareness of the need for information security measures increases.

To succeed on a claim of simple negligence, a plaintiff generally needs to show that (1) the defendant had a duty to use reasonable care, (2) the defendant failed to conform to the required standard and breached that duty of care, (3) a reasonably close causal relationship exists between the conduct and the resulting injury, and (4) as a result of that breach the plaintiff suffered an injury.

a. Duty of Care

The first element of a negligence cause of action—that the defendant owed a duty of care to the plaintiff—is governed by the general doctrine that there is no affirmative duty to act, barring a special relationship between the defendant and plaintiff. Factors used in the determination of whether a special relationship exists include the social interests involved,
the severity of the risk, the burden on the defendant, the likelihood of the occurrence of the risk, and the relationship between the parties.\textsuperscript{165}

Though few courts have found a defendant liable for negligent maintenance of information systems because of limitations discussed below, there is growing recognition of a legal duty to protect sensitive information.\textsuperscript{166} In at least one case, \textit{Remsburg v. Docusearch, Inc.}, a court found that a private investigator or information broker had a “duty to exercise reasonable care” to not reveal a third party’s personal information if the disclosure creates a foreseeable risk of harm to the person whose information is disclosed.\textsuperscript{167}

\textbf{b. Defining the Standard of Care}

A number of commentators believe that a legal standard of care is emerging due to a combination of federal and state regulatory and enforcement actions, as well as court decisions that have imposed on businesses the obligation to take adequate precautions to protect the security of their information systems and the confidentiality of sensitive data transmitted and stored on their systems.\textsuperscript{168} Traditionally, if a duty of care is found, the standard by which the defendant is judged is how a reasonable person would act under similar circumstances.\textsuperscript{169} This standard of care may suffice in a negligence action, particularly where no security precautions are taken. In a recent Michigan case, for example, a union defendant who allowed an employee to take home confidential information without any security measures, in spite of concerns expressed by the executive board to the contrary, was found liable to union members who were victims of identity theft that likely resulted from the theft of their information while in the employee’s possession.\textsuperscript{170}


\textsuperscript{166} See generally Cobell v. Norton, 391 F.3d 251 (D.C. Cir. 2004) (generally affirming the lower court’s finding that the Department of the Interior had breached its management duties by not properly securing the computer system containing information on billions of dollars in Indian trust accounts); Remsberg v. DocuSearch, Inc., 816 A.2d 1001, 1008 (N.H. 2003) (holding that the “risk of criminal misconduct is sufficiently foreseeable so that an investigator has a duty to exercise reasonable care in disclosing a third person’s personal information to a client”).

\textsuperscript{167} \textit{Remsburg}, 816 A.2d at 1001 (finding that an investigation service that discovered the decedent’s work address through a pretextual phone call, and then sold it to another person, was liable for damages to the person deceived, under the N.H. Consumer Protection Act).


\textsuperscript{169} See Restatement (Second) of Torts § 283 (1965).

\textsuperscript{170} \textit{See Bell}, 2005 WL 356306, at *5.
In cases where security precautions have been taken, however, and the issue is one of degree, this standard of care may be difficult to determine. Rather than apply the reasonable person standard of care, courts can adopt a standard of conduct provided by a statute, regulation, or industry practice under the principle of negligence per se. A general standard of care for negligence actions can be derived from the process-oriented approach seen in the FTC’s Safeguards Rule, originally applied to financial institutions subject to the FTC’s jurisdiction, and recently expanded, in practice, if not officially, to cover other businesses. Though not mandating the specific technical measures organizations need to take to meet governmental expectations, this process-oriented approach requires organizations to identify risks, assess the impact of those risks, develop and implement safeguards to mitigate those risks, and periodically test and monitor the effectiveness of security procedures, updating them as necessary.

Questions still remain, however, as to the standard of care that businesses in different industries should meet in their information security practices. The FTC enforcement actions discussed in Part I serve to position the Safeguards Rule as a general standard. Recent statements by the FTC suggest a move to establish a de facto standard for all entities that collect, maintain and transfer, or sell sensitive consumer information. While it may serve to set a minimum baseline standard, more specific industry benchmarks may be needed to ensure adequate security protection. Industry standards already exist in many sectors, including financial services and retail. In addition to the regulations promulgated by the governmental agencies mandated under the GLBA, further security guidance documents, security industry resources, and standard-setting organizations provide direction for the development of industry

171. Restatement (Second) of Torts § 874A cmt. e. Under the doctrine of negligence per se, the common-law tort of negligence is not changed, but the standard of care applied is changed from a general standard to a specific rule of conduct.
172. See supra Part I.B.1.b.
173. See supra notes 68-69 and accompanying text.
174. See Identity Theft Hearing, supra note 70, at 10 (statement of Deborah Platt Majoras, Chairman, FTC) (recommending that the Congress authorize the Commission to extend the Safeguards Rule beyond customer information collected by financial institutions, although acknowledging that Section 5 of the Federal Trade Commission Act already requires companies to secure sensitive data if substantial consumer injury could result from the failure to do so).
175. See generally Freeman, supra note 21, at 9-11 (providing examples of general security standards, such as the National Strategy to Secure Cyberspace, the International Organisation for Economic Co-Operation and Development (OECD), and ISO 17799, a protocol developed by the International Standards Organization).
176. See Kiefer, supra note 15, at 29-30 (describing non-regulatory sources of security obligations arising from industry-wide rules, such as the National Automated Clearing House Association’s rules regarding online debit entries against a Web shopper’s bank account; the Payment Card Industry Data Security Standard, requiring merchants and payment processors to safeguard account data and to protect networks against attack; and Identrus, LLC, setting operating rules and policies for secure business-to-business electronic commerce).
expectations.\textsuperscript{177} Taken as a whole, the regulations lay out the process by which financial institutions should determine which security controls are appropriate for their businesses to secure their computer systems and customer data.

Industry groups, seeking to avoid more burdensome governmental regulation, are working to develop industry-wide standards.\textsuperscript{178} But compliance with industry standards is not necessarily sufficient to meet the standard of care in a negligence action.\textsuperscript{179} Under traditional negligence theory, a defendant is considered negligent if the burden of taking adequate precautions against a foreseeable risk is less than the probability of damage and the gravity of the damage.\textsuperscript{180} If corporations take steps to fulfill compliance requirements, without making a real commitment to information security, they may be exposing themselves to liability.

c. Causation and Harm

Plaintiffs encounter difficulties to recovery under a negligence theory when trying to prove the elements of causation and harm. Causation—that a breach was the proximate cause of the harm to the plaintiff—can be difficult to prove in the case of identity theft where criminals are infrequently caught.\textsuperscript{181} Even if the plaintiff can show harm, the defendant’s negligence may not be the proximate cause in many of these instances. Intervening criminal acts may break the chain of causation so that the

\begin{footnotes}
\item[177] See generally Fed. Fin. Insts. Examination Council, supra note 17. In the financial sector, governmental agencies, such as the Federal Financial Institutions Examination Council (FFIEC), direct businesses and organizations to supplement regulations with agency guidelines, third party information security resources, and standard setting groups. The FFIEC is an interagency body empowered by the Federal Reserve Board, the Federal Deposit Insurance Corporation, the Office of the Comptroller of the Currency, the Office of Thrift Supervision, and the National Credit Union Administration to make recommendations to promote uniformity in the supervision of financial institutions. See FFIEC, http://www.ffiec.gov (last visited Sept. 30, 2006).
\item[179] See The T.J. Hooper v. Northern Barge Corp., 60 F.2d 737 (2d Cir. 1932) (holding that the owner of tugboats was liable to the owners of barges towed by the tugboats and sunk in a storm because he was negligent in not having weather radios on the tugs, even though such radios were not the industry norm).
\item[180] See United States v. Carroll Towing Co., Inc., 159 F.2d 169 (2d Cir. 1947) (expressing the actor’s duty in algebraic terms, where liability depends on whether B (the burden of adequate precautions) is less than P (the probability of a certain event occurring) multiplied by L (the gravity of the injury if the event occurs)).
\item[181] Police departments are not equipped to deal with this type of theft and are reluctant to pursue investigations. Identity Theft Res. Ctr., Identity Theft: The Aftermath 2003, 34 (2003), available at http://www.idtheftcenter.org/idadftermath.pdf (reporting results of a survey that found that only 51% of respondents—the victims of identity theft—had the police take a report during their first contact with the authorities).
\end{footnotes}
defendant's breach of duty is not the legal cause of the injury suffered by the plaintiff.\textsuperscript{182} Additionally, many jurisdictions do not allow plaintiffs to recover for economic losses absent any physical injury, under the economic loss doctrine.\textsuperscript{183} The rationale for this rule is to restrict economic loss claims to breach of warranty or breach of contract claims, and limit liability to those injuries that are foreseeable.\textsuperscript{184} The economic loss doctrine has been applied in varying forms, however, and some courts have shown an indication of moving away from this limitation altogether.\textsuperscript{185}

A recent decision, \textit{Stollenwerk v. Tri-West Healthcare Alliance}, granting a defendant's motion for summary judgment, highlights some of the difficulties plaintiffs can expect to encounter.\textsuperscript{186} The defendant, a government contractor managing the Department of Defense's regional health insurance program, experienced a burglary, but took no subsequent action to secure its facility.\textsuperscript{187} A year and a half later, thieves broke in again and stole computer hard drives containing the plaintiffs' personal information.\textsuperscript{188} Soon afterwards, the personal information of one plaintiff was used in six attempts to open credit card accounts, two of which were successful.\textsuperscript{189} The Arizona Federal District Court held that the plaintiff could not show that the defendant's security measures produced the plaintiff's injury, "'in a natural and continuous sequence, unbroken by any efficient intervening cause.'"\textsuperscript{190} The closeness in time between the burglary and the first attempt at identity theft, though persuasive, was not found to be "dispositive of the causation issue."\textsuperscript{191} Two other plaintiffs, neither the victim of identity theft, sought to recoup the costs of credit

\textsuperscript{182} See Critical Information Infrastructure Protection, \textit{supra} note 36, at 50.
\textsuperscript{183} See, e.g., Spivack \textit{v. Berks Ridge Corp., Inc}, 586 A.2d 402 (Pa. Super. Ct. 1990) (holding that condominium purchasers could not sue real estate developers and builders for alleged defects). In product liability cases, the doctrine is usually applied where damages occur only to the product itself. See \textit{Fidelity & Deposit Co. of Md. v. Int'l Bus. Machs. Co.}, No. 1:05-CV-0461, 2005 WL 2665326, at *1 (M.D. Pa. Oct. 19, 2005) (finding that the economic loss doctrine barred a negligence claim for loss of electronic data due to computer malfunction since the data was considered to be part of the property itself).
\textsuperscript{184} See \textit{Fidelity & Deposit Co. of Md.}, 2005 WL 2665326, at *2-3.
\textsuperscript{185} See, e.g., Indemnity Ins. Co. of N. Am. \textit{v. Am. Aviation, Inc.}, 891 So.2d 532 (Fla. 2004) (applying the economic loss doctrine only in product liability cases or where a party in contractual privity with another seeks to recover tort damages for matters arising from the contract); Neb. Innkeepers, Inc. \textit{v. Pittsburgh-Des Moines Corp.}, 345 N.W.2d 124, 128 (Iowa 1984) (applying the doctrine to all tort claims that fail to show personal injury or property damage); \textit{People Exp. Airlines, Inc. v. Consol. Rail Corp.}, 495 A.2d 107, 118 (N.J. 1985) (holding that economic losses are recoverable if suffered by individuals the defendant knows or has reason to know will likely suffer losses).
\textsuperscript{187} See id. at *1.
\textsuperscript{188} See id.
\textsuperscript{189} Id.
\textsuperscript{190} Id. at *5 (quoting Robertson \textit{v. Sixpence Inns of Am.}, 789 P.2d 1040, 1047 (Ariz. 1990)).
\textsuperscript{191} See id. at *7.
monitoring and identity theft insurance, basing their arguments on a theory analogous to medical monitoring for toxic exposure. While the court seemed willing to consider the analogy, it found that the plaintiffs could not prove actual exposure of sensitive personal information.

Stollenwerk indicates just a few of the obstacles to recovering damages under tort law for an information security breach. Traditional notions of harm and causation will need to be reconsidered in an information security context before a negligence cause of action can provide an adequate remedy to those injured by inadequate security policies and procedures.

2. State Privacy and Breach Notification Laws

States have led the way in enacting breach notification laws and consumer identity theft protection. The purpose of breach notification laws is twofold: to inform consumers when unauthorized individuals have accessed their personal information so they can take precautions to prevent or minimize harm, and to encourage businesses to improve data security to prevent breaches that will trigger consumer notification. Currently, over twenty states have enacted breach notification laws, with varying requirements. Some statutes target only information brokers, while others include any persons doing business in the state. Some statutes provide an express private right of action, while most provide for state enforcement actions. The difficulty in complying with these various requirements has led many commentators and business industry groups to call for a uniform federal notification law.

192. See id. at *3.
193. See id. at *5.
194. See supra Part I.B.2.a.
195. See Data Security Hearing, supra note 144 (statement of Edmund Mierzwinski, Program Director, U.S. Public Interest Research Group).
196. See supra note 104.
197. See, e.g., Ga. Code Ann. § 10-1-911(2) (Supp. 2005) (defining information broker as any person or entity who collects, assembles, evaluates, compiles, reports, transmits, transfers, or communicates data for fees or dues); Me. Rev. Stat. Ann. tit. 10, § 1347(3) (Supp. 2005) (defining information broker similarly except that the entity’s primary purpose is furnishing personal data to nonaffiliated third parties).
198. See, e.g., Del. Code Ann. tit. 6, § 12B-102 (Supp. 2005) (covering any individual or commercial entity that “conducts business in Delaware and that owns or licenses computerized data that includes personal information about a resident of Delaware”).
The starting point for much of the discussion in this area is California’s Breach Notification Law, SB 1386. A number of privacy advocates recommend SB 1386 as the model for future federal legislation, although many industry groups argue that the impact of similar legislation could result in unintended and unwanted effects.

Notification is required when someone has compromised the security, confidentiality, or integrity of state residents’ personal information. Most statutes follow SB 1386’s definition of personal information as an individual’s first name or first initial, last name, and at least a social security number, driver’s license number or state identification card number, or an account number, credit card number, or debit card number in combination with any security code necessary to access a financial account. Some state statutes are more expansive and include additional data elements, such as medical information, date of birth, or mother’s maiden name.

SB 1386 requires notification when unencrypted personal information “was, or has reasonably believed to have been, acquired by an unauthorized person,” and over ten states have followed suit. As an alternative, some states require notification when a business or organization determines there is a likely or reasonable risk of harm to consumers. This “harm

202. See supra notes 99-102 and accompanying text.
203. See Solove & Hooflnagle, supra note 148, at 374; see generally State Pub. Interest Groups and Consumers Union of the U.S., Inc., The Clean Credit and Identity Theft Protection Act: Model State Laws (2005), available at http://www.consumersunion.org/pdf/model.pdf (describing a model act which provides template provisions for state legislatures that are designed to help consumers prevent some of the harm from identity theft). The breach notification is similar to California’s SB 1386 law and requires notice to state residents when any entity that handles, collects, or disseminates personal information when there has been a security breach, as well as allow a civil action by any individual injured by a violation of the statute. See State Pub. Interest Groups and Consumers Union of the U.S., Inc., supra, § 7(B)(1), (D)(1).
204. See Financial Services Hearing, supra note 144 (statement of Ira D. Hammerman, Senior Vice President and General Counsel, Securities Industry Association) (warning that consumers could become desensitized to breach notifications and fail to act on the information).
210. See, e.g., Ark. Code Ann. § 4-110-105 (“Notification under this section is not required if, after a reasonable investigation, the person or business determines that there is no reasonable likelihood of harm to customers.”); Conn. Gen. Stat. Ann. § 36a-701(b) (West Supp. 2006) (requiring no notification in the event of a breach, but only after consultation with federal, state, and local law enforcement agencies).
"trigger" is viewed by many consumer advocates as giving too much discretion to businesses. Additionally, advocates argue that "harm" is often construed narrowly and does not take into account the inconveniences that consumers experience after a security breach. Proponents of this approach warn that without the "harm trigger," consumers will be deluged with breach notices that bear no relation to the risk of actual harm, and may become confused or desensitized to future notices.

Additional issues remain over the question of exemptions to notice. For example, while SB 1386 and most, if not all, state statutes provide a notice exemption for data that is encrypted, they do not specify the level of encryption necessary to exempt the organization. Some privacy advocates argue that, because of weaknesses in encryption technologies, breach notification laws should not exempt encrypted data from breach notification. Others, however, argue that removing the exemption requirement would increase notices of questionable value sent to consumers and also reduce the incentive for businesses to improve security through data encryption.

A number of states exempt financial institutions, subject to the GLBA notification requirements, and health organizations, subject to violations of the Health Insurance Portability and Accountability Act of 1996 (HIPAA), from the notification requirements. Some statutes provide that compliance is not necessary where an entity is covered by an existing

---

211. See Data Security Hearing, supra note 144 (statement of Edmund Mierzwinski, Consumer Program Director, U.S. Public Interest Research Group) (warning that requiring a "harm trigger" may mean that consumers will not be notified after a breach if a business does not know who took the data or why, and citing the example of CitiFinancial, which claimed that the loss of unencrypted backup tapes containing millions of names and Social Security numbers posed little risk of harm to consumers).

212. See, e.g., H.R. 3997 Hearing, supra note 143 (statement of Evan Hendricks, Editor/Publisher, Privacy Times) (arguing against a particular House bill that did not include inconvenience of changing or closing a financial account into its definition of "harm").

213. See, e.g., Financial Services Hearing, supra note 144 (statement of Ira D. Hammerman, Senior Vice President and General Counsel, Securities Industry Association).

214. See, e.g., Cal. Civ. Code § 1798.29 (West Supp. 2006); N.D. Cent. Code § 51-30-01 (Supp. 2005) (defining "personal information" as data elements that are not encrypted); N.C. Gen. Stat. Ann. § 75-65 (2005); see also Skinner, supra note 102, at 45 (noting that the authors of SB 1386 appeared to equate encryption with security, rather than recognizing that encryption is just one component of a security program).


PROTECTING INFORMATION SECURITY

federal or state law if that law provides greater protection to consumers and disclosure requirements that are as thorough.218

Finally, only security breaches involving “computerized data” fall under the notification requirements of SB 1386 and most other statutes; loss of paper records, which still account for the majority of known identity thefts, is covered by a minority of the state breach notification statutes.219

C. Federal Breach Notification Bills

A number of breach bills have been introduced in Congress since 2005, yet Congress has been unable to reach a consensus and is unlikely to enact a bill in the near future.220 Some version of a data security and breach notification legislation will likely emerge, however, as both industry representatives and consumer groups acknowledge the need for federal legislation.221 Aspects of these bills, while similar in many respects, have important differences in the scope of information protected, the trigger for notification and the form it must take, exemptions from notification, penalties, and preemption of state laws.222 These differences are described below.

1. Scope of Protection

How legislation defines “personal information” will impact its applicability in security breach notification. One of the more restrictive bills defines “sensitive personal information” as an individual’s address in addition to the personal information required under SB 1386.223 Another bill defines personal information more broadly as either an individual’s first and last name, address, or phone number.224 Yet another requires “any combination of identifying information that would allow the unauthorized

218. See, e.g., Ark. Code Ann. § 4-110-106 (Supp. 2005) (excluding businesses that are regulated by “a state or federal law that provides greater protection to personal information and at least as thorough disclosure requirements”); Del. Code Ann. tit. 6, § 12B-103(b) (2005).


220. See Tom Zeller, Jr., Waking Up to Recurring ID Nightmares, N.Y. Times, Jan. 9, 2006, at C3 (noting the lack of agreement among industry groups, who want to retain discretion over when to notify consumers of a breach, and consumer groups, who advocate for a broader bill that would preserve existing state laws while implementing broad federal notification requirements).


person to reasonably be able to identify the individual."225 Of course, the more restrictive the definition, the less likely the number of security breaches will require notification.

2. Notification Trigger

The types of breaches that trigger notification differ among the bills. Most require there to be significant or reasonable risk of identity theft to the person whose information has been acquired,226 although some bills call for notification when there has likely been unauthorized access to personal information.227 But even these latter bills provide safe harbors as long as no significant risk of harm exists and the entity notifies the appropriate government agency,228 where compliance could compromise national security or hinder a law enforcement investigation,229 or where the accessed data is encrypted.230

3. Preemption of State Laws

Though security and privacy advocates acknowledge the need for a national standard governing breach notification, some fear that potential federal legislation intended to preempt state laws will dilute the more stringent provisions of these disclosure statutes.231 Opponents of federal regulation alone argue that federal regulation should provide a baseline of security protections, while the states should be able to innovate new privacy protection approaches.232 While some bills propose only partial preemption of state laws,233 others would completely preempt state or local laws involving information security programs or security breach notification rules.234 One bill would go so far as to preempt any “state or local law, regulation, rule, administrative procedure, or judicial precedent” which imposes liability on a business for failure to implement and maintain an

225. S. 768, 109th Cong. § 8(a) (2005).
226. See, e.g., S. 1326 § 3(b)(1); S. 1408 § 3(c); H.R. 3997 § 3(f).
227. See, e.g., S. 1789 § 321(a); S. 768 § 8(a).
228. See, e.g., S. 1789 § 322(b).
229. See, e.g., S. 1789 § 322(a).
230. See, e.g., H.R. 3997, 109th Cong. § 3(f) (2005); S. 768 § 8(a).
231. See supra note 112 and accompanying text.
232. See Solove & Hoofnagle, supra note 148, at 377-78; see also Data Security Hearing, supra note 144 (statement by Edmund Mierzwinski, Consumer Program Director, U.S. Public Interest Research Group) (asserting that “[a] strong argument can be made that the states’ privacy leadership is adequate and continuing”). But see Declan McCullagh, Perspective: Navigating the Law of Unintended Consequences, CNet News.com, Mar. 14, 2005, http://news.com.com/Navigating+the+law+of+unintended+consequences/2010-7348-3-5611746.html (describing state laws whose consequences could prove problematic either because they were written too narrowly or too broadly).
233. See S. 1789 § 304 (preempting any state laws related to protective security measures for personal information).
234. See S. 1326, 109th Cong. § 5 (2005); S. 1408, 109th Cong. § 7 (2005); H.R. 3997 § 6(a).
adequate information security program or notify an individual of any breach of security, effectively precluding common law actions.\textsuperscript{235}

Given the numerous breach notification laws in existence, federal legislation preempting state statutes could undermine current consumer protections. The following section proposes federal legislation which will ensure that businesses take appropriate steps to protect sensitive data while maintaining the protection afforded under state laws.

\section*{III. PROPOSALS FOR FEDERAL LEGISLATION}

Security breaches will continue to occur until businesses find that the costs from inadequate security measures outweigh the investments needed to implement a comprehensive information security plan.\textsuperscript{236} Federal and state governments, along with the courts, can shift this cost-benefit analysis towards better security in the ways discussed below.

\subsection*{A. Maintain GLBA's and FTC's Process-Oriented Approach}

Approaching information security from a risk management perspective, rather than mandating specific technical measures, will lead to more effective information security measures. Any federal legislation should maintain the flexible nature of the process-oriented approach seen in the GLBA-mandated Interagency Guidelines and Safeguards Rule. But federal agencies, such as the FTC, are limited in their resources, so future legislation should not remove the enforcement role of the states from such a regulatory scheme.

The FTC has been successful in pursuing investigations and enforcement actions against companies that have experienced major security breaches.\textsuperscript{237} Although the Commission has made recent moves to expand the Safeguards Rule to nonfinancial institutions whose security practices have caused or could likely cause substantial injury to consumers, Congress should formally extend the FTC's authority to all entities that store electronic data.\textsuperscript{238} In particular, this authority should extend to data brokers and third party processors. Congress should also maintain the Safeguards Rule's process-oriented approach and resist calls to mandate specific technical measures. That responsibility is better left to regulatory agencies, which can provide specific regulations based on the nature of the risks faced by each industry.\textsuperscript{239}

\textsuperscript{235} H.R. 3997 § 6(c) (expressly excluding state trespass, contract, tort, or fraud actions from preemption).
\textsuperscript{236} See Part I.A supra for a discussion of those costs and reasons to improve information security. See also Critical Information Infrastructure Protection, supra note 36, at 43 (noting the need to change the cost-benefit analysis of securing critical infrastructures).
\textsuperscript{237} See supra Part I.B.1.a.
\textsuperscript{238} See supra Part I.B.1.b.
\textsuperscript{239} See generally supra notes 175-77 and accompanying text.
B. Allow Development of Common Law Liability

Common law negligence remedies can serve an important role in providing recourse to injured victims, helping crystallize security standards, and motivating businesses to take reasonable steps to protect their information systems. As more courts acknowledge the responsibility of businesses to “become increasingly vigilant in protecting such information,” and redefine traditional notions of harm, causation, and duties in an information security context, barriers to recovery under a negligence theory for harm caused by lax security practices will fall.

1. Standard of Care

Standards of care must remain flexible to accommodate the range of situations encountered. Applying process-oriented standards, like the FTC’s Safeguards Rule, to a defendant’s conduct will force courts to consider the rationale for a business’s security plan, including reasons for failing to enact certain measures. Overall compliance with industry standards, if they exist, will also need to be considered when determining an appropriate standard of care. A business decision not to follow such standards in light of specific risk factors should be evaluated if those risks materialize and cause harm to third parties.

2. A New Definition of Harm and Causation

To serve tort law’s purposes of providing recourse to injured parties and encouraging risk-mitigating behavior by businesses, courts will need to consider harm and causation differently in an information security context. A proper notion of harm will need to encompass monetary damages, inconvenience, time, and monitoring and insurance costs to third parties. But even if courts are willing to accept new definitions of harm, injured parties will not recover unless the issues posed by security breaches and identity theft are addressed. Many security breaches and instances of identity theft are never solved, leaving injured parties unable to show with absolute certainty that a particular security breach caused their harm.

C. Encourage Disclosure in Information Security

Imposing greater liability on businesses for damage caused by inadequate security procedures could exacerbate the problem of insufficient

241. See supra Part II.B.1.c.
242. See supra note 181 and accompanying text.
243. See supra note 181 and accompanying text.
information disclosure. A federal disclosure law is needed, not just to inform consumers of potential risks and encourage companies to ensure adequate protection, but also to provide information to businesses, organizations, and government on the true scope of the problem for proper risk assessment.

D. Federal Breach Notification Law

Congress should implement security breach legislation, which does not weaken many of the protections already mandated under state laws. Such a law should parallel the majority of state laws and, to avoid overwhelming and (even worse) desensitizing consumers with breach notifications, should require notification where there is a reasonable risk of harm. The determination of what constitutes harm should be made in consultation with federal authorities, as Connecticut’s statute requires, to ensure that corporations provide adequate notification.

Exemptions from notification should include encrypted data to encourage more companies to implement encryption methods. Notification should be required for both paper and electronic data breaches, since loss of paper records still accounts for the majority of known identity thefts.

Most importantly, federal legislation should contain a narrow preemption provision and savings clause similar to the GLBA’s provisions. Only state statutes’ provisions that are inconsistent with federal legislation should be preempted to the extent of the inconsistency. A savings clause should clearly exclude from preemption state statutes that afford greater protection and any state common law causes of action for victims injured by security breaches.

Allowing states to serve as “laborator[ies] . . . and try novel social and economic experiments” to protect data security appears to conflict with calls for a uniform federal standard. Most proposed legislation calls for preemption of state statutes and only one expressly saves common law claims from preemption. While uniformity can lead to more certainty in the courts and decrease costs to businesses, which are no longer liable under state enactments and lawsuits, it shifts the costs of damages to consumers who are not in a position to protect the data maintained by businesses and

245. See supra Part I.A.
246. See supra Part II.B.2, note 204 and accompanying text.
248. See Ponemon, supra note 216 and accompanying text. Concerns over the type of encryption necessary to meet the exemption can be resolved by requiring federal agencies’ regulations to address the issue.
249. See Skinner, supra note 102.
250. See Part I.B.1.a supra for discussion of GLBA’s provisions.
251. See supra notes 109-10 and accompanying text.
254. See H.R. 3997, 109th Cong. §6(c) (2005).
organizations. Requiring corporations to bear the cost of inadequate information security will ensure that affirmative steps are taken to improve security.

CONCLUSION

A strong federal breach notification legislation coupled with the development of a common law tort liability framework for inadequately protecting personal and sensitive consumer information will serve to encourage protection of information systems and assets. Not only does it place the responsibility for protecting this type of data on the entities in the best position to take protective measures, but it will help ensure the growth and reliance on electronic information systems.

255. See Joseph Nocera, Data Theft: How to Fix the Mess, N.Y. Times, July 9, 2005, at C1 (suggesting that the only way to manage the risks and effects of identity theft is by making financial institutions liable for fraudulent transactions).

256. See id.