I/S: A JOURNAL OF LAW AND POLICY FOR THE INFORMATION SOCIETY

MICHAEL E. JONES[*]

Data Breaches: Recent Developments in the Public and Private Sectors

Abstract: In 2007, data breach issues became even more serious than in previous years as breaches continued to occur on a regular basis, threatening the security of over 150 million records. The second biggest data breach ever recorded occurred this past year at the Department of Veterans Affairs, and triggered a flurry of federal activity. This year also saw the initial settlements and resolutions of the ChoicePoint and CardSystems incidents. The issue of data breach continues to evolve rapidly as both the states and the federal government seek to pass legislation and address current issues. This paper provides an update on major data breaches in the past year and examines repercussions from previous incidents, including litigation and settlements. It also reports on proposed and enacted legislation at the state and federal levels.

[*] The author is a 2008 J.D. candidate at The Ohio State University Moritz College of Law. He received a B.S. in Aeronautical and Astronautical Engineering from The Ohio State University in 2005.

I. INTRODUCTION

Keeping private information private has become increasingly difficult. More and more personal data, such as medical information, financial information, and Social Security numbers, are being collected by a wide variety of institutions, from public to financial to educational. The information collected is supposed to remain private and to be used by the collecting institution only. Recently, however, it has become clear that personal information possessed by these institutions may be unwittingly disclosed to third parties. Data breaches were first thrust into the spotlight in 2005, when ChoicePoint, a data brokerage firm, sold the personal information of approximately 145,000 people to criminals posing as a small business.[1] Disclosures of data breach incidents have continued at an increasing rate since the ChoicePoint incident. The Privacy Rights Clearinghouse estimates that, since the ChoicePoint breach, over 166 million individual records containing "sensitive personal information" have been compromised in hundreds of separate data storage breaches.[2]

Several important developments in the area of data breaches occurred in 2006 and 2007. First, major data breaches continued to cause problems across the public and private sectors. Incidents occurred at corporations, public and private educational institutions, and at state and federal government agencies. Second, two issues continued to serve as points of contention in the data breach community: what kind of event should trigger a data breach notification, and what the effects of data encryption might be and whether it should serve as a safe harbor. Third, the federal government created the Identity Theft Task Force and released new Office of Management and Budget ("OMB") guidelines, which instruct federal agencies how to manage data breaches. Additionally, for the first time, the Federal Trade Commission ("FTC") exercised its authority over institutions suffering data breaches by assessing civil

[1] *See* Milton Sutton, Note, *Security Breach Notifications: State Laws, Federal Proposals, and Recommendations*, 2 ISJLP 927, 927 (2006) (background information on the ChoicePoint incident); *see also* Derek Somogy, Note, *Information Brokers and Privacy*, 2 ISJLP 901 (2006).

[2] Privacy Rights Clearinghouse, A Chronology of Data Breaches, Oct. 1, 2007, http://www.privacyrights.org/ar/ChronDataBreaches.htm. *But see* Kenneth Dreifach, *Data Privacy, Web Security, and Attorney General Enforcement*, 865 PLI/PAT 355, 362 (2006) ("Because of data breach security notification laws now in place in more than twenty states . . . numerous other data breaches have been publicized.").

fines and requiring compliance with FTC orders. Furthermore, representatives introduced data breach legislation in both the House and the Senate. Fourth, state legislatures adopted new data breach laws, with Minnesota passing the most prominent data breach notification statute. Finally, in the private sector, corporations confronted the costs associated with preventing and discovering data breaches, and private individuals initiated the first lawsuits against corporations that suffered a data breach. This article addresses each of these developments in depth and provides insight as to their effects, as well as recommendations for the future.

II. DATA BREACH INCIDENTS

Although one author dubbed 2006 to be "the year of the data breach,"[3] 2007 may contend for that title, as the rate of data breaches increased through 2007. Institutions affected by such breaches ranged from federal and state government agencies to educational institutions to private corporations. The major causes of these breaches varied with the type of institution suffering the breach. A report issued by the American Association of Retired Persons ("AARP"), which studied data breach incidents from January 1, 2005, to May 26, 2006, indicated that government data breaches are primarily the result of physical theft of electronic storage devices and the accidental publication of personal information to the Internet.[4] Educational institutions, on the other hand, suffered over half their data breaches at the hands of hackers.[5] Nearly forty-three percent of all data breaches that were reported during this period involved educational institutions.[6] This underlines the importance to security administrators of determining their institution's susceptibility to a specific method of data breach.

[3] Beth Gautier, *The Year of the Data Breach - 2006 Dramatically Changed the Identity Theft Landscape*, KROLL, Dec. 27, 2006, http://www.krollfraudsolutions.com/media-center/press-release6.aspx.

[4] NEAL G. WALTERS, AARP PUBLIC POLICY INSTITUTE, INTO THE BREACH: SECURITY BREACHES AND IDENTITY 3 (2006), *available at* http://assets.aarp.org/rgcenter/consume/dd142_security_breach.pdf.

[5] *Id.*

[6] *Id.*

A. STATE GOVERNMENT

In March 2006, the Ohio Secretary of State accidentally posted the Social Security numbers of residents who made purchases using credit cards or received bank loans on state websites where such records are searchable by the public.[7] One month later, in April, the state of Ohio accidentally sent the Social Security numbers of possibly millions of Ohio voters to approximately twenty political campaigns.[8] The information was accidentally recorded on CDs that were supposed to contain only voter registration information for the campaigns to use for telephone calls and canvassing.[9] In June 2006, the state of Minnesota compromised the security of tax information of approximately 2,400 individuals and 48,000 businesses.[10]

B. FEDERAL GOVERNMENT

In May 2006, in what was the second largest overall breach at the time, the Department of Veteran Affairs ("VA") lost personally identifiable information of more than 26 million United States veterans.[11] The information was stored unencrypted on a laptop that an employee had taken home without proper authorization.[12] The laptop was then stolen from the employee's home.[13] Although the records did not contain any health or financial information, the data did include the Social Security numbers and birth dates of every living veteran who served after 1974, as well as data on some of the veterans'

[7] Todd Weiss, *Ohio Secretary of State Sued Over ID Info Posted Online*, COMPUTERWORLD, Mar. 3, 2006, http://www.computerworld.com/databasetopics/data/story/0,10801,109213,00.html.

[8] Todd Weiss, *Ohio Recalls Voter Registration CDs; Social Security Numbers Included*, COMPUTERWORLD, Apr. 28, 2006, http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=110983.

[9] *Id.*

[10] Herón Márquez Estrada, *State Taxpayer Data Lost in Mail*, MINNEAPOLIS-ST. PAUL STAR TRIB., June 29, 2006, *available at* http://www.startribune.com/462/story/520906.html.

[11] Terry Frieden, et al., *Source: Theft of Vets' Data Kept Secret for 19 Days*, CNN.COM, May 23, 2006, http://www.cnn.com/2006/US/05/23/vets.data/index.html.

[12] *Id.*

[13] *Id.*

spouses.[14] In response, the only immediate steps taken by the VA was to mail letters to veterans[15] and to create a website providing information about the incident.[16]

The situation was made even more difficult because the government waited nineteen days to notify veterans that their personal information had been compromised.[17] This delay occurred because the government was faced with the choice of notifying the veterans immediately, which could tip off the laptop thieves as to the information they were carrying, or delaying notification in the hopes that the information could be recovered.[18] The choice to delay notification resulted in a backlash against the government as veterans had to wait over two and a half weeks to take any steps to protect themselves.[19] Senator Patrick Leahy (D-VT) called the delay "unacceptable," and pointed out that the VA should have provided veterans with free credit monitoring services to monitor their credit reports for fraudulent activity.[20] VA Secretary Jim Nicholson said he was outraged by the VA's decision not to immediately disclose the breach.[21]

Other government agencies have been affected by data breaches as well.[22] In fact, since 2003, all nineteen United States government

[14] *Id.*

[15] Letter from R. James Nicholson, Sec'y, U.S. Dep't of Veterans Affairs, to Veterans (June 5, 2006), http://www.firstgov.gov/veteransinfo_letter.shtml.

[16] *See* USA.gov, Latest Information on Veterans Affairs Data Security, http://www.usa.gov/veteransinfo.shtml (last visited Jan. 5, 2008) [hereinafter Information on Veterans Affairs]. The site answers frequently asked questions and provides veterans with information on what steps they can take to protect themselves from damages.

[17] Frieden, s*upra* note 11.

[18] *Id.*

[19] *Id.*

[20] Press Release, U.S. Senator Patrick Leahy, 'A Heckuva Bad Job for America's Veterans': Reaction of Senator Patrick Leahy to the Delay of Notification of Veterans' Data Breach (May 23, 2006), *available at* http://leahy.senate.gov/press/200605/052306b.html.

[21] *VA Chief 'Outraged' by Delay in Revealing Theft of Veterans' Data*, FOX NEWS.COM, May 24, 2006, http://www.foxnews.com/story/0,2933,196800,00.html.

[22] *See*, *e.g.*, Brian Koerner, *Data Breach at the Federal Trade Commission*, ABOUT.COM, June 22, 2006, http://idtheft.about.com/b/a/256579.htm; USDA Possible Personal Information Breach, http://www.usa.gov/usdainfo.shtml (last visited Jan. 5, 2008).

agencies have reported at least one breach of personal information under their control.[23] In October 2006, the House Government Reform Committee released a report giving the federal government a D-plus in breach management after reviewing federal data breach incidents.[24] The committee's findings emphasize the importance of physical data security. Indeed, one of the biggest sources of data breaches is lost or stolen laptops that contain personal information; over 1,100 have been stolen, lost, or reported missing since 2001.[25]

C. EDUCATIONAL INSTITUTIONS

Beginning in October 2005, hackers broke into a central University of California – Los Angeles ("UCLA") database that stored records for approximately 800,000 former and current students and staff.[26] The hackers had access until November 2006, when their activities were finally noticed.[27] UCLA notified persons whose data may have been compromised through a letter sent on December 12, 2006.[28] One former student reported that someone had stolen her identity and taken out a $24,500 car loan in her name[29] using her old UCLA address in order to obtain the loan.[30] However, UCLA officials claimed they have no evidence the data was misused.[31] The outcome of this case may be significant, as actual damages following a data breach have

[23] Linda Rosencrance, *Report: Data Loss Widespread at Government Agencies*, COMPUTERWORLD, Oct. 16, 2006, http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9004168.

[24] Bill Brenner, *Feds Get a D Plus for Data Security*, SEARCHSECURITY.COM, Oct. 19, 2006, http://searchsecurity.techtarget.com/originalContent/0,289142,sid14_gci1225321,00.html.

[25] Rosencrance, *supra* note 23.

[26] *FBI Looks into UCLA Hacking Case*, CBS2.COM, Dec. 13, 2006, http://cbs2.com/local/UCLA.Computer.Hacker.2.525820.html.

[27] *Id.*

[28] *See* Letter from Norman Abrams, Acting Chancellor, UCLA, to potential identity theft victims (Dec. 12, 2006), *available at* http://www.identityalert.ucla.edu/ID_alert_letter.pdf.

[29] *FBI Looks into UCLA Hacking Case*, *supra* note 26.

[30] *Id.*

[31] *Id.*

been difficult to prove.[32] The university has established an identity alert webpage suggesting that affected persons place a fraud alert on their credit files.[33] The site further suggests that those affected should take advantage of their federal right to one free credit report per year from each credit reporting agency and should stagger their requests to activate up-to-date monitoring without incurring costs.[34] However, nowhere does the university offer any monetary assistance to affected persons to help pay for monitoring their accounts.[35]

Ohio University suffered a similar data breach when one of its databases was breached for thirteen months, in a manner similar to the UCLA incident.[36] This occurred because the university decommissioned a network server, excluding it from all patches and security updates, but failed to actually take it offline.[37] The university set up a website for the over 300,000 affected alumni and friends whose information may have been stolen from the server.[38] Ohio University, like UCLA, recommends that those affected place a fraud alert on their credit files.[39]

III. NOTIFICATION TRIGGERS AND ENCRYPTION: TWO POINTS OF CONTENTION

To properly examine any data breach legislation, it is first important to understand the two main points of contention: determining what sort of breach triggers a legal requirement to notify

[32] Jaikumar Vijayan, *Court Dismisses Lawsuit in Merchant Data-Breach Case*, COMPUTERWORLD, June 23, 2006, available at http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9001391.

[33] *See* UCLA Identity Alert, http://www.identityalert.ucla.edu (last visited Jan. 5, 2008).

[34] *Id.*

[35] *Id.*

[36] Brian Koerner, *Ohio University Data Breach*, ABOUT.COM, http://idtheft.about.com/od/2006/p/Ohio_data_theft.htm (last visited Jan. 5, 2008).

[37] *Id.*

[38] Data Theft and Identity Protection at Ohio University, http://www.ohio.edu/datatheft (last visited Jan. 5, 2008) [hereinafter Ohio University Website].

[39] *Id.*

consumers, and whether encryption serves as a safe harbor. This section provides an overview of both topics.

A. NOTIFICATION TRIGGER

One of the most significant issues regarding data breaches is how to properly notify individuals whose personal information has become compromised. The issue involves determining what constitutes a breach and which types of breaches should trigger notification. Before current and proposed legislation can be examined, however, it is important to understand the two types of triggers that most commonly appear in these laws: the acquisition-based trigger, and the risk-based trigger.

The acquisition trigger is best illustrated by California's data breach notification law. This type of trigger is used by almost half of the states with breach notification laws.[40] The California law, which is the strictest of any state law, provides that notification is required after any data breach if "the personal information was, or is reasonably believed to have been, acquired by an unauthorized person."[41] The law further provides that "disclosure shall be made in the most expedient time possible and without unreasonable delay."[42] This language is used in other state notification laws as well.[43] The most important feature of this trigger is that it requires no evidence that an unauthorized person actually acquired the data. It was under this type of trigger that ChoicePoint, a Georgia corporation, first made its data breach public pursuant to California law, a state in which ChoicePoint does business.[44]

[40] State PIRG Summary of State Security Freeze and Security Breach Notification Laws, July 18, 2006, http://www.pirg.org/consumer/credit/statelaws.htm [hereinafter *State PIRG Summary*]. Thirty-four states have breach notification laws. The sixteen states that use an acquisition trigger are: California, Delaware, Florida, Georgia, Hawaii, Illinois, Indiana, Maine, Minnesota, Nevada, New York, North Dakota, Oklahoma, Rhode Island, Tennessee, and Texas. *Id.*

[41] CAL CIV. CODE § 1798.29(a) (West 2006).

[42] *Id.*

[43] *E.g.*, H.R. 6191 (R.I. 2005); S.B. 122 (Tex. 2005).

[44] It is important to note the effect of the California law on businesses throughout the U.S. Because corporations doing business in California must follow this law, it has become a de facto standard across the country. The Privacy Rights Clearinghouse estimates that of the millions of records that have been compromised due to data breaches, the California law is responsible for bringing the majority of these to light. Beth Givens, the director of the Privacy

The benefit of the acquisition trigger is that consumers are made aware of *potential* breaches of their information. A few scholars, however, fear it results in too much reporting. Fred Cate, law professor and director of the Center for Applied Cybersecurity Research at Indiana University in Bloomington, has concerns about using a low trigger, like the acquisition trigger.[45] According to Cate "[t]he threat of identity theft from data losses is being greatly exaggerated, and that's because a lot of people have fallen into the trap of equating data loss with identity theft."[46] Cate is worried that low triggers overstate the problem, which will make the response to serious threats less effective; "it's like the boy who cried wolf."[47] Cate's prediction appears to be accurate. Greg MacSweeney, editor-in-chief of *Wall Street & Technology* magazine, commented "some pretty major personal data thefts are buried deep in the papers."[48] MacSweeney noted that E*Trade Financial lost $18 million and TD Ameritrade lost $4 million due to the same identity theft scam, yet "the media coverage was … virtually nonexistent."[49]

The other common trigger is the "risk-based" trigger, which is generally less favorable to consumers and friendlier to businesses. It limits the notification to only those situations where a risk assessment determines that a danger exists to those whose records were breached. Eighteen states currently use some form of a risk-based trigger.[50] The current Ohio law uses such a trigger; it requires both a reasonable belief that information was acquired, and that the acquisition of such

Rights Clearinghouse, stated that the California law is "an extraordinarily important law." She further hints at the law's influence in stating that she "doubt[s] we'd have very much to report to consumers if it weren't for this law." David Lazarus, *New Bid to Protect Your Data*, S.F. CHRON., Jan. 12, 2007, *available at* http://www.sfgate.com/cgi-bin/article.cgi?f=/c/a/2007/01/12/BUGSPNHB4T1.DTL.

[45] Steve Lohr, *Surging Losses, But Few Victims in Data Breaches*, N.Y. TIMES, Sept. 27, 2006, *available at* http://www.nytimes.com/2006/09/27/technology/circuits/27lost.html?ex=1165122000&en=d710f1a149b7bd35&ei=50700.

[46] *Id.*

[47] *Id.* (citing Cate).

[48] Posting of Greg MacSweeney to Wall Street & Technology: Blog, http://www.wallstreetandtech.com/blog/archives/2006/11/when_risk_manag.html (Nov. 29, 2006, 12:16 EST).

[49] *Id.*

[50] *State PIRG Summary*, *supra* note 40.

information "will cause a material risk of identity theft or other fraud."[51] It should also be noted that the risk-based trigger may not uniformly apply to all breaches like the California trigger that many states have adopted. For instance, New Jersey's Identity Theft Prevention Act does not require notification when "the business or public entity establishes that misuse of the information is not reasonably possible."[52]

B. ENCRYPTION

As of July 2006, no state required data custodians to provide notification of a data breach if the compromised information is encrypted.[53] Thus, corporations can avoid being subject to notification requirements by simply encrypting all electronically stored data. Although encryption may seem expensive, Avivah Litan, Vice President of Gartner Inc., testified in a congressional hearing that data protection is much less costly than data breaches.[54] Litan estimates that encryption will cost $5 per account the first year and $1 per account each additional year.[55] She contrasts that with the $79 per account that ChoicePoint had to spend as a result of its data breach.[56] If Litan's estimate is correct, then an ounce of preventative encryption is truly worth a pound of notification. Litan recommends looking to the Payment Card Industry's encryption standards as a guide for developing future federal encryption standards.[57]

[51] H.B. 104, 126th Gen. Assem., Reg. Sess. (Ohio 2005).

[52] 2005 N.J. Laws 226.

[53] Bruce E. H. Johnson et al., *Data Breach Notice Legislation: New Technologies and New Privacy Duties?,* 865 PLI/PAT 203, 216 (2006).

[54] *Data Protection is Much Less Costly than Data Breaches: Hearing Before the H. Comm. on Veterans Affairs*, (2006) (statement of Avivah Litan, Vice President, Gartner, Inc.), *available at* http://veterans.house.gov/hearings/schedule109/may06/5-25-06/AvivahLitan.html.

[55] *Id.*

[56] *Id.*

[57] *Id. See also* PCI SECURITY STANDARDS COUNCIL, PAYMENT CARD INDUSTRY DATA SECURITY STANDARD (2006) (requirement four addresses data encryption), *available at* https://www.pcisecuritystandards.org/pdfs/pci_dss_v1-1.pdf.

The encryption safe harbor is favored by data brokerage firms.[58] They argue that encrypted information poses no threat, even if it falls into the hands of identity thieves, and therefore there is no need to disclose a breach of encrypted information.[59] The federal government also favors the encryption of all personal information records, as indicated in a June memorandum from the OMB.[60] The memo recommends that all agencies and departments "[e]ncrypt all data on mobile computers/devices which carry agency data unless the data is determined to be non-sensitive, in writing, by your Deputy Secretary."[61] The goal of the recommendation is to compensate for the lack of physical security protections used when private information is dealt with outside of the agency.[62] Privacy writer Dennis Fisher praises the move, calling it necessary, as he believes government agencies do not treat personal information as carefully as corporations.[63] Fisher believes that private companies are not likely to

[58] Caron Carlson, *Storm Brews Over Encryption 'Safe Harbor' in Data Breach Bills*, EWEEK.COM, May 31, 2005, http://www.eweek.com/article2/0,1895,1822182,00.asp.

[59] *Id.* At first glance, it may seem odd that some of the parties pushing for an encryption safe harbor are also ones who may be lagging behind the federal government when it comes to full-disk encryption. Those opposed to encryption safe harbors argue that this discrepancy is due to the notion that establishing a safe harbor for encryption discourages corporations from being forward-thinking in other data security measures. Bruce Schneier, Chief Technology Officer at Counterpane Internet Security, Inc. states "[y]ou can encrypt the data with a trivial algorithm and get around [the law]," meaning that a cursory method of encryption would satisfy the law, but do little to protect the data. In contrast, proponents of encryption contend that hesitation to encrypt is due to the fear that full disk encryption would slow network traffic and applications. Instead, systems should perform encryption carefully to avoid slowdowns, but in such a way that they still encrypt important information. *See* Carlson, *supra* note 58; Paul F. Roberts, *MCI Data Theft Intensifies Encryption Debate*, EWEEK.COM, May 31, 2005, http://www.eweek.com/article2/0,1895,1821333,00.asp.

[60] Memorandum from Clay Johnson III, Deputy Dir. for Mgmt. of the Office of Management and Budget, to the Heads of Dep'ts and Agencies 1 (June 23, 2006), *available at* http://www.whitehouse.gov/omb/memoranda/fy2006/m06-16.pdf.

[61] *Id.*

[62] *Id.*

[63] Dennis Fisher, *Federal Government Pushes Full-Disk Encryption*, SEARCHSECURITY.COM, Jan. 10, 2007, http://searchsecurity.techtarget.com/columnItem/0,294698,sid14_gci1238490,00.html ("A lost laptop full of IRS records doesn't translate into lost revenue, it just means bad press.").

move to full disk encryption until required to by the government because of their concerns about short-term costs.[64]

Some analysts, including Adam Golodner, oppose mandatory encryption, especially in situations where data is not merely stored, but is accessed frequently for use in consumer transactions.[65] Golodner, a former member of the White House E-Commerce Working Group, and currently serving as a director in the Global Security and Technology Policy division of Cisco Systems, states that encryption is something to be determined by the market.[66] Golodner opines that "market responses are generally the most powerful, efficient, and efficacious way to address the issue."[67] Moreover, Golodner states that the first vendors to adopt security standards such as encryption could secure a competitive advantage, leading competitors to do the same.[68] Additionally, he stresses that implementation of mandatory policies such as encryption can have unintended consequences.[69] Cisco could be harmed by a mandatory encryption policy, as it has already taken steps in accordance with its own innovation to secure its information.[70] Golodner suggests that adopting mandatory encryption could actually cause a well-developed system, like Cisco's, to be less secure, and potentially could discourage innovation.[71]

[64] *Id.* ("The problem is that the accumulated bad publicity and fines aren't nearly enough to force companies to infringe on the productivity gains that mobile devices provide.").

[65] *See* Adam Golodner, Address to the Progress and Freedom Foundation's Data and Security Summit (May 10, 2006), *in* PROGRESS ON POINT, Nov. 2006, *available at* http://www.pff.org/issues-pubs/pops/pop13.30securitysummittranscript.pdf.

[66] Biography of Adam Golodner, Director of Global Security and Technology Policy for Cisco Systems, http://www.cisco.com/warp/public/779/govtaffairs/images/Adam_G_bio.pdf (last visited Jan. 5, 2008). (Mr. Golodner was also the Associate Director for Policy at the Institute for Security and Technology Studies at Dartmouth College); S. W. Smith, *A Funny Thing Happened on the Way to the Marketplace*, IEEE SEC. AND PRIVACY MAG., Nov/Dec 2003, at 74, *available at* http://www.cs.dartmouth.edu/~sws/pubs/marketplace.pdf (search on "Golodner").

[67] Smith, *supra* note 66, at 78.

[68] *Id.* at 77.

[69] *Id.* at 77–78. *See also* Golodner, *supra* note 65.

[70] Golodner, *supra* note 65, at 78.

[71] *Id.*

IV. FEDERAL DEVELOPMENTS

Federal developments have been significant in two areas. First, in April 2007, the Identity Theft Task Force released its strategic plan for combating identity theft,[72] and worked with the OMB to develop a memorandum that was sent to all federal agencies instructing them how to safeguard data and handle data breach incidents.[73] Second, Congress is continuing its efforts to enact data breach legislation.

Before discussing these items, it is important to recognize the few existing federal laws that address the issue of data breaches. Currently, protection for electronic information is required in four specific areas. Health information is protected by the Security Rule of the Health Insurance Portability and Accountability Act ("HIPAA"), which requires healthcare entities to protect against reasonably anticipated threats to the security of stored information and to protect against unauthorized uses or disclosures of such information.[74] Financial institutions are required to protect the data they possess under the FTC's Safeguards Rule.[75] Violations of the rule, as well as unfair and deceptive trade practices, can result in FTC action. After the exercise of such action, in 2006 the FTC reached settlements with ChoicePoint[76] and CardSystems Solutions.[77] Consumers' personal

[72] THE PRESIDENT'S IDENTITY THEFT TASK FORCE, COMBATING IDENTITY THEFT: A STRATEGIC PLAN (Apr. 2007), *available at* http://www.identitytheft.gov/reports/StrategicPlan.pdf.

[73] Memorandum from Clay Johnson III, Office of Mgmt. and Budget, to the Heads of Dep'ts and Agencies (May 22, 2007), *available at* http://www.whitehouse.gov/omb/memoranda/fy2007/m07-16.pdf.

[74] 45 C.F.R. § 164.306(a) (2006). For more information on HIPAA, *see* Sharona Hoffman & Andy Podgurski, *In Sickness, Health, and Cyberspace: Protecting the Security of Electronic Private Health Information*, 48 B.C. L. REV. 331 (2007).

[75] 15 U.S.C.S. §§ 41–58 (LexisNexis 2007). For more information on the FTC's authority to regulate under the Safeguard Rule, *see* Benita A. Kahn & Heather J. Enlow, *The Federal Trade Commission's Expansion of the Safeguards Rule*, 54-SEP .FED. LAW. 39 (2007).

[76] ChoicePoint had been charged under the Fair Credit Reporting Act with making consumer credit history available to unauthorized persons and with failing to maintain procedures to verify the identity of such persons. ChoicePoint agreed to pay $10 million in civil damages to the FTC, the largest judgment in FTC history, with an additional $5 million in consumer redress. Under the terms of the settlement, ChoicePoint must establish and maintain a comprehensive data security program. ChoicePoint also must be audited biennially for the next twenty years by a qualified, independent, third-party professional. Press Release, FTC, ChoicePoint Settles Data Security Breach Charges; To Pay $10 Million in Civil Penalties, $5 Million for Consumer Redress (Jan. 26 2006), *available at* http://www.ftc.gov/opa/2006/01/choicepoint.htm. To view a copy of the court judgment, *see*

financial information is protected by the Gramm-Leach-Bliley Act.[78] Finally, information gathered online about children under the age of thirteen is protected by the Children's Online Privacy Protection Act ("COPPA").[79]

A. THE PRESIDENT'S IDENTITY THEFT TASK FORCE AND THE OMB GUIDELINES

In the wake of the VA data breach, President George W. Bush issued an Executive Order to create an Identity Theft Task Force to determine guidelines on how to "improve the effectiveness and efficiency of the Federal Government's activities in the areas of identity theft awareness, prevention, detection, and prosecution."[80] The task force includes the chairman of the FTC, the United States Attorney General, and the Secretary of Veterans Affairs, among others.[81] In an interim report, the task force noted that it is "almost inevitable" that federal agencies will experience data breaches.[82] With

United States v. ChoicePoint, Inc., No. 06-0198, (N.D. Ga. 2006), *available at* http://www.ftc.gov/os/caselist/choicepoint/0523069stip.pdf. Most important, perhaps, was that ChoicePoint was charged with violating the unfairness prong of the Federal Trade Commission Act, which makes it unlawful to engage in "unfair or deceptive acts or practices in or affecting commerce." 15 U.S.C. § 45 (2006).

[77] Although CardSystems was not subject to civil penalties as ChoicePoint was, it was similarly required to undergo audits every two years for the next twenty years. As with ChoicePoint, CardSystems is also required to establish and maintain a comprehensive information security program. Press Release, FTC, CardSystems Solutions Settles FTC Charges (Feb. 23, 2006), *available at* http://www.ftc.gov/opa/2006/02/cardsystems_r.shtm. For more information on CardSystems, *see* Tom Krazit, *Security Breach May Have Exposed 40M Credit Cards*, IDG NEWS SERV., June 17, 2005, http://www.computerworld.com/databasetopics/data/story/0,10801,102631,00.html.

[78] Gramm-Leach-Bliley Act, Pub. L. No. 106-102, 113 Stat. 1338 (1999). For more information on the Gramm-Leach-Bliley Act, see Christopher Wolf, *2005 Overview of the Gramm-Leach-Bliley Act*, 828 PLI/PAT 761 (2005).

[79] For more information on COPPA, *see* Marcy E. Peek, *Information Privacy and Corporate Power: Towards a Re-imagination of Information Privacy Law*, 37 SETON HALL L. REV. 127, 151 (2006).

[80] Exec. Order No. 13,402, 71 C.F.R. § 27945 (2006).

[81] *Id.* § 2(b).

[82] Jaikumar Vijayan, *Court Dismisses Lawsuit in Merchant Data-Breach Case*, COMPUTERWORLD, June 23, 2006, *available at* http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9001391.

this in mind, the task force developed a strategic plan to combat identity theft.[83] The plan identifies three stages of identity theft: 1) the attempt to steal personal information, 2) the attempt to misuse acquired information, and 3) the harming of the victim.[84] The task force also worked with the OMB to develop a memorandum to federal agencies outlining data security measures and breach notification procedures.[85] The most important aspect of the memorandum is that it required all federal agencies to adopt a breach notification policy by September 22, 2007.[86] Agencies are required to use a "best judgment standard" in developing their breach notification procedures.[87] This standard is intended to be flexible and recognizes that one piece of personally identifiable information may be sensitive at multiple levels, depending on the context.[88]

The memo includes four attachments that outline the notification policy. The first emphasizes agencies' responsibilities to safeguard information under existing law, and also requires a reduction in the use of Social Security numbers and the encryption of all sensitive information stored on devices carrying agency information.[89] The second attachment requires that every federal agency data breach be reported internally to the United States Computer Emergency Readiness Team ("US-CERT") within one hour of identifying that a breach has or may have occurred.[90] The third attachment provides guidance to assist agencies in developing an external notification procedure,[91] including six elements they are expected to consider: 1) whether breach notification is required; 2) the timeliness of the

[83] THE PRESIDENT'S IDENTITY THEFT TASK FORCE, *supra*, note 72.

[84] *Id.* at 12–13. Of particular relevance to this note is the first stage, which often results in a data breach.

[85] Memorandum from Clay Johnson III, *supra* note 73. A risk-based decision framework flowchart was in an earlier version of the memo, available at http://www.whitehouse.gov/omb/memoranda/fy2006/task_force_theft_memo.pdf, at 11.

[86] Memorandum from Clay Johnson III, *supra* note 73, at 1.

[87] *Id.* at 1, note 6.

[88] *Id.*

[89] *Id*. at 7.

[90] *Id*. at 9.

[91] *Id*. at 12.

notification; 3) the source of the notification; 4) the contents of the notification; 5) the means of providing the notification; and 6) who receives the notification.[92]

Additionally, in determining whether breach notification is required, the agency must consider five specific factors: 1) the nature of the data elements breached; 2) the number of individuals affected; 3) the likelihood the information is accessible and useable; 4) the likelihood the breach may lead to harm; and 5) the ability of the agency to mitigate the risk of harm.[93] The fourth and final attachment includes the OMB's new Rules and Consequences policy, which emphasizes that managers, supervisors, and employees are all responsible for safeguarding personally identifiable information.[94] The policy notes that an individual's failure to act in accordance with the OMB guidelines is a serious offense and can result in the individual being reprimanded, suspended, removed, or otherwise disciplined in accordance with agency policy.[95]

B. Federal Legislation

The OMB guidelines provided a rigorous framework for the development of breach notification procedures within federal agencies, however the same cannot be said for private entities. Currently, no relevant federal legislation concerning data breaches involving private entities has passed Congress.

In the wake of the VA incident, numerous bills were introduced in the 109th Congress in 2006, but the session ended without any legislation being passed.[96] The issue continued to draw attention in the 110th Congress, where at least ten bills regarding data breach notification have been introduced; however, none of the bills have

[92] *Id*. at 13.

[93] *Id*. at 14–15.

[94] *Id*. at 21.

[95] *Id*. at 22.

[96] *See*, *e.g.*, Veterans Identity and Credit Security Act of 2006, H.R. 5835, 109th Cong. (2006); Data Accountability and Trust Act, H.R. 4127, 109th Cong. (2006); Financial Data Protection Act, H.R. 3997, 109th Cong. (2006); Identity Theft Protection Act, S. 1408, 109th Cong. (2006); Personal Data Privacy and Security Act, S. 1789, 109th Cong. (2005); Data Security Act, S. 3568, 109th Cong. (2006).

been sent to committee.[97] Notably, of the proposed legislation, only two bills have been reported to the Senate: the Personal Data Privacy and Security Act of 2007 and the Notification of Risk to Personal Data Act of 2007.

The most critical issues facing federal legislators are the same as those facing the states: the notification trigger and the possibility of an encryption safe harbor. Under current law, states have the freedom to take individual approaches to these two issues. Recently, however, the issues have attracted the attention of federal legislators, and may eventually be subject to preemption by federal law. Further complicating federal efforts, is the issue of determining who bears the responsibility of enforcing any new federal law.

The current round of proposed legislation takes a more refined approach in determining the magnitude and severity of a data breach than the bills proposed in the 109th Congress. Bills proposed in 2006 did not address the number of records affected, and attempted, without success, to apply one-size-fits-all standards to both large and small breaches.[98] This additional refinement enhances the sophistication of the notification trigger; instead of being simply risk-based or acquisition-based, the notification trigger considers the context of the breach. For example, under the Cyber-Security Enhancement and Consumer Data Protection Act of 2007, the trigger has two tiers:[99] if information about more than 10,000 individuals is compromised, the trigger is acquisition-based;[100] if information about fewer than 10,000

[97] Data Security Act of 2007, H.R. 1685, 110th Cong. (2007); Data Security Act of 2007, S. 1620, 110th Cong. (2007) (bill mirrors H.R. 1685); Cyber-Security Enhancement and Consumer Data Protection Act of 2007, H.R. 836, 110th Cong. (2007); Personal Data Protection Act of 2007, S. 1202, 110th Cong. (2007); Data Accountability and Trust Act, H.R. 958, 110th Cong. (2007); Personal Data Privacy and Security Act, S. 495, 110th Cong. (2007); Notification of Risk to Personal Data Act of 2007, S. 239, 110th Cong. (2007); Federal Agency Data Breach Protection Act, S. 1558, 110th Cong. (2007); Federal Agency Data Breach Protection Act, H.R. 2124, 110th Cong. (2007) (similar to S. 1558); Identity Theft Protection Act, S. 1178, 110th Cong. (2007).

[98] *See*, *e.g.*, Veterans Identity and Credit Security Act of 2006, H.R. 5835, 109th Cong. (2006); Data Accountability and Trust Act, H.R. 4127, 109th Cong. (2006); Financial Data Protection Act, H.R. 3997, 109th Cong. (2006); Identity Theft Protection Act, S. 1408, 109th Cong. (2006); Personal Data Privacy and Security Act, S. 1789, 109th Cong. (2005); Data Security Act, S. 3568, 109th Cong. (2006).

[99] Cyber-Security Enhancement and Consumer Data Protection Act of 2007, H.R. 836, 110th Cong. § 1039 (2007).

[100] *Id.*

individuals is involved, the more stringent risk-based trigger is used.[101] As a result, customers involved in large breaches may receive better protection than those involved in small breaches. This disparity in protection could serve to balance the interests of business, who find notification to be time-consuming and expensive, with the interests of consumers, who want to know when their information has been compromised.

The two-tiered approach is used in a different way by the Identity Theft Protection Act ("ITPA").[102] Under the ITPA, a risk-based trigger is used for all data breaches, but if the breach affects more than 1,000 individuals, the breached entity must notify the consumer credit reporting agencies.[103] Stated another way, the breached entity has no duty to notify the consumer credit reporting agencies if the breach affects fewer than 1,000 individuals and the entity can show that there is no reasonable risk of identity theft due to the breach.[104] However, this bill is limited in scope since it applies only to entities that have a direct relationship with consumers.[105]

The Federal Agency Data Breach Protection Act,[106] introduced in the House and Senate, and the Notification of Risk to Personal Data Act of 2007, as reported in the Senate,[107] use yet another approach to the notification trigger in an attempt to balance consumer and entity interests. These bills set the default to the less stringent acquisition-based trigger unless the entity chooses to perform a risk assessment, in which case the more stringent risk-based trigger is used.[108] If, however, the entity determines from the risk assessment that there is "no significant risk that [the] security breach has resulted in, or will result in, harm to the individuals whose sensitive personally

[101] *Id.*

[102] Identity Theft Protection Act, S. 1178, 110th Cong. (2007).

[103] *Id.* § 3(a).

[104] *Id.* § 3(b).

[105] *Id.* § 3(c)(2).

[106] Federal Agency Data Breach Protection Act, H.R. 2124, 110th Cong. (2007); Federal Agency Data Breach Protection Act, S. 1558, 110th Cong. (2007).

[107] Notification of Risk to Personal Data Act of 2007, S. 239, 110th Cong. (2007).

[108] *Id.*

identifiable information was subject to the security breach," then no notification is required.[109]

The proposed bills contain various terms that address encryption, but, in general, encryption is approached in one of three ways: 1) by exemption, 2) by rebuttable presumption, or 3) as a factor. An exemption provision creates a safe harbor for data that is encrypted; no notification is required if encrypted data is breached. A rebuttable presumption provision creates a rebuttable presumption that no risk exists if encrypted data is breached; no notification is required unless harm is proven to exist. In factor provisions, encryption is treated as merely a factor to consider when assessing the risk to individuals whose records were breached.

Three bills contain specific exemptions for encrypted data, based on the theory that encrypted data is neither usable nor personally identifiable.[110] This approach frees the entity from its duty to notify.[111] Six other bills contain rebuttable presumption provisions that allow the breached entity to operate under the assumption that there is no likelihood of harm.[112] Finally, one bill contains no safe harbors or rebuttable presumptions, but considers encryption as one factor to use in determining whether harm will reasonably result from the breach.[113]

Consumer advocates generally favor federal legislation that includes an acquisition-based trigger[114] and that preempts less

[109] *Id.*

[110] Two of the bills containing a safe harbor for data that is encrypted are the companion Data Security Act of 2007 bills introduced simultaneously in the House and Senate. Data Security Act of 2007, H.R. 1685, 110th Cong. (2007); Data Security Act of 2007, S. 1620, 110th Cong. (2007) (bill mirrors H.R. 1685); Personal Data Protection Act of 2007, S. 1202, 110th Cong. (2007).

[111] H.R. 1685; S. 1202; S. 1620.

[112] Cyber-Security Enhancement and Consumer Data Protection Act of 2007, H.R. 836, 110th Cong. (2007); Data Accountability and Trust Act, H.R. 958, 110th Cong. (2007); Federal Agency Data Breach Protection Act, H.R. 2124, 110th Cong. (2007); Notification of Risk to Personal Data Act of 2007, S. 239, 110th Cong. (2007); Personal Data Privacy and Security Act, S. 495, 110th Cong. (2007) (bill mirrors S. 1558); Federal Agency Data Breach Protection Act, S. 1558, 110th Cong. (2007).

[113] Identity Theft Protection Act, S. 1178, 110th Cong. (2007). This bill also limits notification to situations where there is a direct relationship between the entity suffering the breach and the consumer. *Id.*

[114] Roy Mark, *Groups Slam Data Breach Notification Bill*, INTERNETNEWS.COM, Mar. 17, 2006, http://www.internetnews.com/security/article.php/3592416 ("We think consumers

stringent state laws. Among those who favor a risk-based trigger, however, there remains a divide between those who would have federal legislation preempt state law and those who would not. Proponents of preemption emphasize that a federal law would provide greater uniformity by imposing a national standard and simplifying compliance, especially among companies that do business in multiple states.[115]

Congress has also struggled with inter-committee turf battles over which committee should be responsible for handling data breach legislation.[116] In 2006, data breach legislation was sent to a number of different congressional committees, including the House Judiciary Committee, the House Committee on Financial Services, the House Commerce Committee, the Senate Judiciary Committee, the Senate Commerce Committee,[117] and the Senate Committee on Banking, Housing, and Urban Affairs.[118] Since no committee is specifically tasked with addressing information technology issues, it has largely been up to the individual committees to determine who will be first to push a data breach bill through Congress. Such a feat would, in all likelihood, expand the focus and power of that committee to address future technology issues.

V. STATE DEVELOPMENTS

While the federal government struggles to adopt any sort of national standard through federal legislation, states continue to push data breach bills through their legislatures. In 2006, thirteen states passed data breach notification legislation, bringing the total number

should be notified in case of a breach and it shouldn't be left to the companies to decide.") (quoting Susanna Montezemolo, a policy analyst with Consumers Union).

[115] *See*, *Data Protection and the Consumer: Who Loses When Your Data Takes a Hike?: Hearing Before the H. Subcomm. on Regulatory Reform and Oversight*, 109th Cong. 16–18 (2006), *available at* http://bulk.resource.org/gpo.gov/hearings/109h/28741.pdf (statement of Steve DelBianco, Vice President for Public Policy at the Association for Competitive Technology).

[116] *See* Tory Newmyer, *Data Security Bill Mired in Turf Battle*, ROLL CALL (Aug. 7, 2006).

[117] Roy Mark, *Data Breach Bills Crowding Commerce*, INTERNETNEWS.COM, May 12, 2006, http://www.internetnews.com/bus-news/article.php/3605666.

[118] Veterans Privacy Protection Act of 2006, S. 3176, 109th Cong. (2006).

of states with notification laws to thirty-four.[119] In 2007, bills dealing with data breaches were introduced in at least twenty-six other states.[120] Arguably, the most significant piece of state data breach legislation was enacted by Minnesota.[121] That bill creates two safeguards for electronically stored information. The first, which took effect on August 1, 2007, prohibits entities conducting business in Minnesota from retaining credit card data for more than forty-eight hours.[122] The second, which takes effect August 1, 2008, allows financial institutions to recover costs associated with "reasonable actions undertaken by the financial institution as a result of the breach in order to protect the information of its cardholders."[123]

Reasonable actions include canceling or reissuing credit cards, closing accounts, taking other actions to stop payment or block transactions, opening or re-opening accounts affected by the breach, refunding or crediting a cardholder for the cost of any unauthorized transaction, and, finally, notifying cardholders affected by the breach.[124] Although this legislation does not provide a direct method of recovery for consumers whose information has been compromised, it does hold the breached entity liable for costs borne by financial institutions. This liability may encourage those institutions to provide compensation to their members.

Connecticut, Illinois, Massachusetts, and Texas have proposed similar legislation.[125] The Connecticut House passed a bill that was

[119] Nat'l Conf. of State Legislatures, 2006 Breach of Information Legislation, http://www.ncsl.org/programs/lis/cip/priv/breach06.htm (last visited Jan. 5, 2008). Arizona, Colorado, Hawaii, Idaho, Illinois, Indiana, Kansas, Maine, Nebraska, New Hampshire, Utah, Vermont, and Wisconsin all passed legislation in 2006. *Id.*

[120] Nat'l Conf. of State Legislatures, 2007 Breach of Information Legislation, http://www.ncsl.org/programs/lis/cip/priv/breach07.htm (last visited Jan. 5, 2008).

[121] 2007 Minn. Sess. Law Serv. ch. 108 (H.F. 1758) (West) (codified at MINN. STAT. § 325E.64 and taking effect on August 1, 2007).

[122] *Id.*

[123] *Id.*

[124] *Id.* subdiv. 3.

[125] Posting of Randy Gainer to Privacy and Security Law Blog, http://www.privsecblog.com/archives/security-breaches-state-laws-to-shift-some-data-breach-costs-to-businesses-with-weak-security.html (May 25, 2007).

similar to Minnesota's law,[126] but the Connecticut Senate removed the recovery provisions altogether.[127] The Connecticut bill, now devoid of data breach references, was adopted by the legislature on July 11, 2007.[128] The Illinois bill was nearly identical to the new Minnesota law in scope and in allowing costs to be recovered by financial institutions.[129] The Massachusetts legislature passed several bills. One bill was analogous to Minnesota's and allowed financial institutions to recoup their costs,[130] while others purposefully excluded such a provision.[131] The Texas version required that businesses accepting credit cards comply with all Payment Card Industry ("PCI") Data Security Standards ("DSS") requirements,[132] which recommend that credit card data be retained for no longer than 48 hours.[133] The Texas bill also allowed recovery in the same manner as the new Minnesota law.[134] One important difference, however, is that the Texas bill excluded financial institutions from the requirement to adopt the PCI DSS standards.[135]

V. PRIVATE SECTOR

Although the private sector remains focused on the data breach legislation battles in Congress, it is also concerned with more practical matters. In 2007, one of the biggest issues the private sector faced was the effect of data breaches on corporate costs. These costs arise in two

[126] S.B. 1089 (substitute), Gen. Assem., 2007 Reg. Sess. (Conn. 2007) (as reported to the Senate Committee on Judiciary).

[127] S.B. 1089, Gen. Assem., 2007 Reg. Sess. (Conn. 2007) (as signed into law).

[128] *Id.*

[129] S.B. 1675, 95th Gen. Assem., 1st Reg. Sess. (Ill. 2007).

[130] H. 213, 186th Gen. Ct., Reg. Sess. (Mass. 2007).

[131] Gainer, *supra* note 125.

[132] H.B. 3222, 80th Leg., Reg. Sess. (Tex. 2007); *see also* PCI SEC. STANDARDS COUNCIL, PAYMENT CARD INDUSTRY(PCI) DATA SECURITY STANDARD 4 (2006), https://www.pcisecuritystandards.org/pdfs/pci_dss_v1-1.pdf.

[133] PCI SEC. STANDARDS COUNCIL, *supra* note 132.

[134] H.B. 3222.

[135] *Id.*

areas: data breach prevention and data breach remediation. As legislation is passed and higher standards are enacted, corporations must spend more money in responding to breaches. Costs result from a variety of remedial actions such as "printing and postage of notification letters, hiring a law firm to address legal issues, offering credit monitoring subscriptions to customers, implementing a customer support hotline and contract call center, as well as customer defections."[136]

The Ponemon Institute, a research organization "dedicated to advancing privacy and data protection practices,"[137] estimates the cost of a data breach at $182 per compromised record, a thirty-one percent increase from 2005.[138] Cost estimates vary greatly, however. In an email to CNET News, Forrester Research stated that a data breach costs the breached entity between $90 and $305 per record.[139] This estimate varies depending upon the type of breach and the regulations that apply, and was based on a survey of twenty-eight companies that experienced data breaches.[140] Darwin Professional Underwriters, a technology liability insurance company, has developed an online calculator for determining how much a data breach would cost.[141] The calculator uses a proprietary algorithm based on breach data reported in the media and other industry resources, including the Ponemon Institute study.[142] Testing of the calculator indicates, not surprisingly, that the cost per breach decreases as the number of records breached increases. At 250,000 records breached, the highest allowable input, the cost per affected record is $51.42. When 1,000 records are affected, the cost per record is $166.27. Some analysts, like Avivah

[136] *Id.*

[137] The Ponemon Institute, http://www.ponemon.org/about.html (last visited Jan. 5, 2008).

[138] Robert Westervelt, *Survey: Data Breach Costs Surge*, SEARCHSECURITY.COM, Oct. 31, 2006, http://searchsecurity.techtarget.com/originalContent/0,289142,sid14_gci1227119,00.html.

[139] Joris Evers, *What's the Cost of a Data Breach?*, CNET NEWS BLOG, April 13, 2007, http://news.com.com/8301-10784_3-6176074-7.html.

[140] *Id.*

[141] Identity Theft Data Loss Cost Calculator, http://www.tech-404.com/calculator.html (last visited Jan 5., 2008).

[142] *Id.*

Litan, have questioned whether these estimates are inflated.[143] Litan, an analyst at Gartner, Inc., responded to the calculator results stating: "I wouldn't bet my house or my enterprise on these numbers. A lot of the costs are often exaggerated."[144]

One important factor in cost determination is the notification trigger. If a low trigger were adopted, it could prove to be expensive for businesses. First, it would require massive amounts of corporate oversight to ensure that every possible breach was recognized. This has proven to be difficult for many corporations. According to the Ponemon Institute, only fifty-nine percent of companies believe they can effectively detect a data breach.[145] Second, it can be difficult to distinguish real breaches from false alarms. False positive rates can run as high as thirty-five percent, affecting an organization's ability to accurately detect a real breach.[146] Small data breaches, ones with fewer than a hundred files, are the most troublesome for companies, as they are likely to be detected only fifty-one percent of the time.[147] In fact, thirty-five percent of organizations cited excessive cost as a reason for not using technology to prevent data breaches.[148]

The Chairman of the Ponemon Institute, Dr. Larry Ponemon, stated that

> [I]n spite of the increased attention being paid to the issue of data security, enormous gaps remain in corporate America's ability to effectively protect sensitive data, and that a lack of

[143] Jaikumar Vijayan, *Just How Much Will that Data Breach Cost Your Company?*, COMPUTERWORLD.COM, April 11, 2007, http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9016296.

[144] *Id.*

[145] Press Release, Ponemon Institute, Ponemon Institute Study Shows Lack of Accountability, Resources at Root of U.S. Corporate Data Loss Problem 1 (Aug. 28, 2006), http://www.ponemon.org/press/Ponemon_Port_AuthorityDetectPr.pdf [hereinafter Ponemon Institute]. *See also* Bill Brenner, *Survey: Data Breaches Difficult to Spot, Prevent*, SEARCHSECURITY.COM, Aug. 31, 2006, http://searchsecurity.techtarget.com/originalContent/0,289142,sid14_gci1213621,00.html.

[146] Ponemon Institute, *supra* note 145, at 1.

[147] *Id.*

[148] *Id.*

> accountability as well as a dearth of resources dedicated to the problem are at the root of the problem.[149]

The most troublesome conclusion of the study, however, is that sixty-three percent of corporations surveyed said they would not be able to prevent future data breaches.[150] If data breaches are truly unpreventable, there is an even more urgent need to establish procedures for reacting to a breach, including notification of those affected.

Even more costs arise once a data breach has been detected. These costs include the postage to send notification letters, legal fees to defend against impending litigation, and the cost to remedy the source of the breach. For example, ChoicePoint reported $11.5 million in costs directly related to the breach, as well as a post-breach decrease of $720 million in its market capitalization.[151] Large-scale data breaches additionally carry implied litigation costs, but since plaintiffs have yet to prevail in recovering damages from breached corporations, these costs will likely be limited to attorney's fees.[152]

VI. Recommendations and Conclusion

While Congress has stagnated, federal agencies, state governments, and the private sector have all made significant advances in developing data breach policies and procedures. The OMB guidelines provide a very clear structure for federal agencies to use when developing data breach policies. In general, individuals whose information is stored by a federal agency should feel protected. Even if a breach were to occur, the OMB guidelines would ensure that US-CERT is notified, the

[149] *Id.*

[150] *Id.*

[151] Brian Koerner, *The Cost of a Data Breach*, ABOUT.COM, http://idtheft.about.com/od/databreaches/qt/Breach_Costs.htm (last visited Jan. 5, 2008).

[152] *E.g.*, Banknorth, N.A. v. BJ's Wholesale Club, 442 F. Supp. 2d 206, 213-214 (M.D. Pa. 2006) (holding that the economic loss doctrine applies to data breach cases, and there can be no recovery for negligence claims based solely on economic damages); Forbes v. Wells Fargo Bank, 420 F. Supp. 2d 1018, 1021 (D. Minn. 2006) (holding that the time and money spent monitoring do not constitute recoverable damages, but rather that "[the defendants'] expenditure of time and money was not the result of any present injury, but rather the anticipation of future injury." For a thorough review of litigation arising out of data breaches, see Stephen Ambrose Jr., Joseph W. Gelb, & Walter E. Zalenski, *Survey of Significant Consumer Privacy Litigation in the United States in 2006*, 62 BUS. LAW. 651 (2007).

individual is notified, and the cause of the breach addressed. However, in addition to the OMB requirements, agencies should adopt sensible breach notification policies that protect the interests of the affected individuals.

Ultimately, the biggest concern is whether individuals will be notified when data stored at a corporation has been breached. Absent congressional consensus on the issue, it is left to state governments and corporations themselves to decide how to handle a data breach. As the cost analysis indicates, it seems cheaper for corporations to be proactive in their efforts to prevent data breaches rather than wait until something happens and hope for the best. However, being proactive requires up-front costs that the corporation may not want to pay. Due to the lack of any law requiring notification in the event of a breach of any stored piece of digital information, consumers should still be wary that they may not be notified should their information end up in the wrong hands. This is especially true in states employing a risk-based trigger that puts the burden on the corporation to decide whether or not to notify individuals.

The risk-based trigger appears problematic because it leaves the notification decision to the breached institution, which may put its own interests ahead of the affected individuals. Therefore, Congress should strive to develop federal laws that employ an acquisition-based trigger. This type of trigger would effectively require corporations to invest in safeguarding data before a breach occurs, rather than afterwards. As cost estimates have shown, this is an economically justifiable move, and it stands to keep costs low even in the face of a consumer-friendly trigger. However, because such a law would require the safeguarding of corporate data, it should also provide an exemption for information that can be shown to be unusable if breached, either due to encryption or other proprietary methods the corporation may developed. The most feasible exemption option would be to employ a rebuttable presumption that the breach of unusable information poses no harm to consumers.

It is apparent that while data breaches continue to be a serious privacy issue, recent developments in the federal, state, and private sectors have provided individuals with a base amount of security. The rate at which data breaches occur seems likely to increase for the coming years, and the burden will remain on information-storing entities to begin to safeguard data more effectively. Nonetheless, increased legislative effort and focused media attention should leave consumers feeling more confident that their private information will remain private.