Washington University Journal of Law & Policy

Volume 32 *New Directions in Environmental Law*

January 2010

# Data Breach Notification Laws: An Argument for a Comprehensive Federal Law to Protect Consumer Data

Jill Joerling
*Washington University School of Law*

# Data Breach Notification Laws: An Argument for a Comprehensive Federal Law to Protect Consumer Data

Jill Joerling*

## INTRODUCTION

During the past four years, over 354,140,197 pieces of personal identifying information have been compromised as a result of data breaches.[1] These breaches have imposed a huge financial burden on both companies and consumers.[2] As a result, forty-six states have enacted legislation seeking to protect consumers by requiring companies to notify them when their personal information is compromised as the result of a data breach.[3] This notification allows consumers to take action to protect their information from identity theft.[4]

---

* J.D. (2010), Washington University School of Law; B.A. (2006), English Literature and Religious Studies, University of Virginia. I would like to thank my family for their support and advice. Additional thanks to my fellow editors and the staff of the *Washington University Journal of Law & Policy* for their hard work and enthusiasm.

1. *See* Privacy Rights Clearinghouse, Chronology of Data Breaches, http://privacyrights.org/ar/ChronDataBreaches.htm CP (last visited May 7, 2010).

2. One study, released by the Ponemon Institute in October 2006, found that information losses to U.S. companies "averaged $182 per lost customer record, an increase of 30 percent over 2005 results. The average total cost per reporting company was $4.8 million per breach and ranged from $226,000 to $22 million." PONEMON INSTITUTE, 2006 ANNUAL STUDY: COST OF A DATA BREACH (2006), http://download.egp.com/pdfs/Ponemon2-Breach-Survey_061020_F.pdf. *See also* Tech//404, Tech//404 Data Loss Cost Calculator, http://www.tech-404.com/calculator.html (last visited Oct. 22, 2009) (providing the estimated cost of a breach based on number of affected records).

3. *See infra* note 34.

4. *See Consumer Survey on Data Breach Notification*, 2008 JAVELIN STRATEGY & RESEARCH, *available at* http://www.docstoc.com/docs/952213/2620_/Javelin-Research-Consumer-Survey-Data-Breach-Notification-June-2008. "[W]hile notification allows the consumer to take protective action and to monitor their accounts more closely, from a customer service perspective, it is to the advantage of the institution to be proactive and offer assistance on behalf of the customer, especially if the exposed data is highly sensitive." *Id.*

This Note argues that existing state laws do not adequately address data security breaches and recommends comprehensive federal data breach notification legislation. Part I provides a brief history of data security breaches precipitating the enactment of data breach notification legislation and an overview of current state data breach notification laws and previously proposed federal legislation. Part II critiques current data breach legislation and outlines the need for federal legislation. Part III proposes guidelines for a federal statute.

## I. HISTORY

### *A. ChoicePoint and the Data Breaches Precipitating Reform*

In February 2005, data collector ChoicePoint[5] revealed that it had mistakenly disclosed the private information of over 145,000 United States residents.[6] While this was not the first reported data breach,[7] the large number of individuals affected elevated the event into the national spotlight.[8] The breach occurred when scammers posed as

5. *See* Grant Gross, *ChoicePoint's Error Sparks Talk of ID Theft Law*, NETWORKWORLD, Feb. 23, 2005, http://www.networkworld.com/news/2005/0223choicerror.html. Among other services, ChoicePoint provides background check documents for business and government agencies hiring workers. The company has access to roughly 19 billion public records and has information on virtually every adult living in the United States. *Id. See also* Bob Sullivan, *Data Theft Affects 145,000 Nationwide: Suspect Arrested in ChoicePoint Case Agrees to Plea Deal*, MSNBC, Feb. 18, 2005, http://www.msnbc.msn.com/id/6979897.

6. *See* Grant Gross, *ChoicePoint to Pay $15 Million for Data Breach*, NETWORKWORLD, Jan. 26, 2006, http://www.networkworld.com/news/2006/012606-choicepoint.html. In the months following the breach, the number of individuals affected was revealed to be closer to 163,000. At least 750 of these individuals were the victims of identity theft as a result of the breach. *Id. See also* Sullivan, *supra* note 5.

7. *See* Ethan Preston & Paul Turner, *The Global Rise of a Duty to Disclose Information Security Breaches*, 22 J. MARSHALL J. COMPUTER & INFO. L. 457, 459 (2004) (describing the first reported data breach that took place at the Stephen P. Teale Data Center in Sacramento, California, on April 5, 2002, when intruders hacked into systems granting access to state employees' personal information).

8. *See, e.g.*, Joseph Menn & David Colker, *More Victims in Scam Will Be Alerted; ChoicePoint Says It Will Notify 110,000 People Outside of California of the Security Breach*, L.A. TIMES, Feb. 17, 2005, at C1; Robert O'Harrow Jr., *ID Theft Scam Hits D.C. Area Residents; 4,500 Caught Up in Loss of Data Conned From Firm*, WASH. POST, Feb. 21, 2005, at A01; John Waggoner, *ID Theft Scam Spreads across USA*, USA TODAY, Feb. 22, 2005, at 1A; Lorene Yue, *ID Theft Warnings for Illinois; Personal-data Fraud Threatens 5,000 Here*,

legitimate businesses in order to gain access to the company's databases, which contained a wide variety of consumer data including names, addresses, Social Security numbers, driver's license numbers, credit reports, and public information such as bankruptcies, liens, and professional licenses.[9] The affected individuals were notified of the breach because of a California law that required notification to California residents.[10] At first the company disclosed the breach only to California residents, but eventually it opted to notify all affected victims.[11]

In the month after news of ChoicePoint's breach became public, Bank of America,[12] PayMaxx,[13] DSW,[14] and LexisNexis[15] each disclosed data breaches. Combined, it was revealed that the breaches compromised 1,502,000 individuals' personal information.[16] In the following years, many additional breaches have been disclosed.[17] A

---

CHICAGO TRIB**.** Feb. 22, 2005, at C01; *Database Company Issues Identity Theft Alert*, N.Y. TIMES, Feb. 27, 2005, at 14CN.

9. *See* Sullivan, *supra* note 5; Gross, *supra* note 5.

10. *See* California Security Breach Information Act, CAL. CIV. CODE §§ 1798.29, 1798.82–.84 (West 2009); Bob Sullivan, *Database Giant Gives Access to Fake Firms: ChoicePoint Warns More than 30,000 They May Be at Risk*, MSNBC, Feb. 18, 2005, http://www.msnbc.msn.com/id/6969799.

11. *See* Nat'l Conference of State Legislatures, Breach of Information, http://www.ncsl.org/IssuesResearch/TelecommunicationsInformationTechnology/OverviewSecruityBreaches/tabid/13481/default.aspx; Sullivan, *supra* note 5.

12. *See* Chronology of Data Breaches, *supra* note 1. On February 25, 2005, Bank of America revealed that 1,200,000 pieces of personal information had been jeopardized as the result of a lost backup tape. *Id.*

13. *See id.* On February 25, 2005, PayMaxx revealed that it had exposed 25,000 customers' personal information online. *Id.*

14. *See id.* On March 8, 2005, DSW disclosed that 100,000 records of personal information had been exposed through a hacking incident. *Id.*

15. *See id.* On March 10, 2005, LexisNexis reported that compromised passwords had exposed information on 32,000 individuals. It was later disclosed that the information of an additional 280,000 individuals also had been compromised. *Id.*

16. *See* Chronology of Data Breaches, *supra* note 1.

17. As of March 2008, the ten largest data breaches were HM Revenue and Customs (affecting 25 million consumers on November 20, 2007), TD Ameritrade (affecting 6.3 million consumers on September 14, 2007), Fidelity National Information Services (affecting 8.5 million consumers on July 3, 2007), Dai Nippon Printing Company (affecting 8.6 million consumers on March 12, 2007), TJX Companies, Inc. (affecting 94 million consumers on January 17, 2007), U.S. Department of Veteran Affairs (affecting 26.5 million consumers on May 22, 2007), Visa, MasterCard, and American Express (affecting 40 million consumers on June 19, 2005), Citigroup (30 million consumers on June 6, 2005), America Online (affecting 30 million consumers on June 24, 2004), Data Processors International (affecting 5 million

disproportionately high number of these breaches have occurred at hospitals and universities.[18] In 2006, public concern over the safety of information stored by government entities was raised[19] when the Department of Veterans Affairs revealed that it had suffered a breach that compromised the data of more than 28,650,000 active duty personnel and veterans.[20] Following the Department of Veterans Affairs breach, in an attempt to standardize government breach response, the U.S. Government Accountability Office issued a report containing recommendations to federal agencies for dealing with data breaches.[21]

---

consumers on March 6, 2003). 10 Largest Data Breaches Since 2000—Millions Affected, http://flowingdata.com/2008/03/14/10-largest-data-breaches-since-2000-millions-affected/ (Mar. 14, 2008).

18. *See* Privacy Rights Clearinghouse, Chronology of Data Breaches 2006: Analysis, http://www.privacyrights.org/ar/DataBreaches2006-Analysis.htm (last visited Feb. 1, 2010). In 2006 private sector breaches made up only fifteen percent of the data breaches caused by outside hackers. Breaches in higher education, medical centers, and the public sector made up fifty-two percent, three percent, and thirteen percent of these breaches, respectively. *Id.* Between 2005 and 2008, education-related data breaches accounted for nearly a third of all data breach incidents. At least 324 breaches were reported by educational institutions during this period, resulting in over twelve million pieces of compromised data. *See* JOSEPH E. CAMPANA, HOW SAFE ARE WE IN OUR SCHOOLS? 2 (2008), http://www.jcampana.com/JCampana Documents/EducationSectorDataBreachStudy.pdf; *see also* Andy Guess, *Data Breaches Hit More Campuses*, INSIDE HIGHER ED., Feb. 12, 2008, http://www.insidehighered.com/news/2008/02/12/breach.

19. *See* Roy Mark, *VA Data Breach Stirs Washington*, INTERNETNEWS.COM, May 23, 2006 http://www.internetnews.com/bus-news/article.php/3608411. In the months following the breach, the Department of Veterans Affairs revealed that two other security breaches had occurred in the past twelve months and had been kept quiet. The Department of Transportation, the Justice Department, the Navy, and other Government entities proceeded to reveal their own data breaches and the lack of security in their systems. *See* Martin H. Bosworth, *Government Scrambles to Secure Data After Breaches*, CONSUMERAFFAIRS.COM, Aug. 16, 2006 http://www.consumeraffairs.com/news04/2006/08/govt_data.html.

20. The information was jeopardized when a laptop that contained the names, birthdates and social security numbers of millions of veterans, was stolen from an employee's home. *See* Press Release, U.S. Dep't of Veterans Affairs, A Statement from the Dep't of Veterans Affairs (May 22, 2006), *available at* http://www1.va.gov/opa/pressrel/pressrelease.cfm?id=1123. The laptop was later recovered. *See* Press Release, U.S. Dep't of Justice, Latest Info. on Veterans Affairs Data Security: Stolen Laptop and External Hard Drive Recovered (June 29, 2006), http://www.sanantonio.gov/veterans/pdf/ObLatstInfo-VetAffairsDataSecurity7.pdf.

21. *See* Jon Brodkin, *GAO Report Targets Data Breach Guidelines*, NETWORKWORLD, Apr. 30, 2007, http://www.networkworld.com/news/2007/043007-gao-data-breach-guidelines.html. The report identified these "lessons learned" from the VA data breach regarding how and when to notify government officials, affected individuals, and the public following a breach: rapid internal notification of key government officials is critical; because incidents vary, a core group of senior officials should be designated to make a decision about an agency's response;

### *B. California's Data Security Law*

On July 1, 2003, California enacted the country's first data breach notification law.[22] The law requires that companies, nonprofit organizations, and government agencies notify California consumers if their personal information is compromised by unauthorized access.[23] This early notification allows consumers to protect themselves against identity theft and mitigate damages resulting from unauthorized access to their information.[24]

---

mechanisms should be in place to collect contact information for affected individuals; determining when to offer credit monitoring to affected individuals requires risk-based management decisions; interaction with the public requires careful coordination and can be resource-intensive; internal training and awareness are critical to timely breach response; contractor responsibilities in data breach response should always be clearly defined. U.S. GOV'T ACCOUNTABILITY OFFICE, REPORT TO CONGRESSIONAL REQUESTERS, PRIVACY: LESSONS LEARNED ABOUT DATA BREACH NOTIFICATION (2007), http://www.gao.gov/new.items/d07657.pdf. The report urged the Office of Management and Budget to develop guidelines for agencies to reduce the risk of identity theft from data breaches. Many of these "lessons" had been addressed in previous guidance from the Office of Management and Budget.

This guidance, set forth by the President's Identity Theft Task Force, consisted of three related recommendations: (1) Agencies should identify a core response group that can be convened in the event of a breach; (2) If an incident occurs, the core response group should engage in a risk analysis to determine whether the incident poses problems related to identity theft; (3) If it is determined that an identity theft risk is present, the agency should tailor its response (which may include advice to those potentially affected, services the agency may provide to those affected, and public notice) to the nature and scope of the risk presented. *See id.* at 21. The GAO recommended further guidance to ensure that the agency determinations regarding when to offer credit monitoring are consistent. OFFICE OF MGMT. & BUDGET, EXEC. OFFICE OF THE PRESIDENT, MEMORANDUM FROM THE IDENTITY THEFT TASK FORCE (2006), http://www.whitehouse.gov/omb/memoranda/fy2006/task_force_theft_memo.pdf.

22. *See* Privacy Rights Clearinghouse, California Security Breach Notification Law Goes Into Effect July 1, 2003, http://www.privacyrights.org/ar/SecurityBreach.htmn (last visited Feb. 1, 2010); California Security Breach Information Act, CAL. CIV. CODE §§ 1798.29, 1798.82–.84 (West 2009). California has consistently been a leader in information security. In 2001, the state opened the California Office of Privacy Protection, the first state agency "dedicated to promoting and protecting the privacy rights of consumers." California Office of Information Security & Privacy Protection, Welcome to the Office of Privacy Protection, http://www.oispp.ca.gov/consumer_privacy/ (last visited Feb. 1, 2010).

23. California Security Breach Information Act § 1798.29.

24. *See* Privacy Rights Clearinghouse, California Security Breach Notification Law Goes Into Effect July 1, 2003, http://www.privacyrights.org/ar/SecurityBreach.htm (last visited Feb. 1, 2010). In response to the law's enactment, Beth Givens of the Privacy Rights Clearinghouse stated:

> in the past, companies usually did not notify their customers when their electronic data had been compromised, subsequently leaving them at risk for identity theft or financial fraud. Now individuals can take the appropriate proactive steps to safeguard their

Under California's Security Breach Information Act, a security breach is defined as the "unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the person or business."[25] Personal information is defined as an individual's first name or initial and last name, in combination with either individual's: (1) the Social Security number; (2) driver's license or identification number; or (3) account number, debit, or credit card number, together with any required access code "that would permit access to an individual's financial account."[26] The law has been amended to protect medical information and health insurance information as well.[27] A company that has experienced a security breach must make the disclosure in the "most expedient time possible and without unreasonable delay."[28] This notice can be delayed when a law enforcement agency determines that the notification will impede a criminal investigation.[29] Notification may be provided to consumers in writing or electronically.[30] However, if the company can demonstrate that the cost of providing notice would exceed $250,000, that the affected class of subject persons exceeds 500,000, or that the company does not have sufficient contact information, then the company can rely on

---

> financial healthy when they learn that their information may have been accessed by hackers or unauthorized employees. . . . This law mandates good corporate stewardship of customer information, not just for businesses located in California, but for any entity that has personal information about Californians.

*Id.*

25. California Security Breach Information Act § 1798.82(d). *See also* Jeffrey M. Rawitz & Alexander Frid, *Security Breach Notification Requirements: Guidelines and Securities Law Considerations*, JONES DAY COMMENTARIES, Mar. 2006, http://www.jonesday.com/pubs/pubs_detail.aspx?pubID=S3225.

26. California Security Breach Information Act § 1798.29(e).

27. *See id.* § 1798.29(e)(4); *see also* Edgar D. Bueno, John L. Nicholson & Melissa M. Starry, *California's Data Breach Notification Law Now Covers Medical and Health Insurance Information*, PILLSBURY WINTHROP SHAW PITTMAN CLIENT ALERT, Jan 14, 2008, http://www.pillsburylaw.com/siteFiles/Publications/1D256A2125E5D9C778C456728A64B27D.pdf.

28. California Security Breach Information Act § 1798.29(a); Rawitz & Frid, *supra* note 25. Although not stated in the statute, California's guidelines on breach notification recommend that entities notify consumers of the security breach within ten business days of discovery. Alan Mansfield, *Is Your Client Prepared to Comply With the Data Security Breach Notification Laws?*, ABTL REPORT, Spring 2007, http://www.abtl.org/report/sd/abtl-report-spring-2007.pdf.

29. *See* California Security Breach Information Act § 1798.82(c).

30. *Id.* § 1798.82(g)(1)–(2).

substitute notification methods to comply with this requirement.[31] Substitute notice consists of e-mail notice, conspicuous posting of the notice on the company's website, and notification in a major statewide medium.[32]

### *C. Other State Data Breach Notification Laws*

In the years since California enacted its law, forty-six states and the District of Columbia have followed its lead and enacted laws of their own.[33] Many of these laws are substantially similar to the California law; however, there are significant differences as well.[34] Variances in applicability; exemptions; notification procedures and timelines; and enforcement can create difficulties for companies attempting to comply with the various laws following a breach.[35]

#### 1. Applicability

After a data breach is discovered, affected companies are forced to determine which, if any, of the many state data breach notification laws are triggered based on the information that has been compromised. California's Security Breach Information Act applies only to data records stored electronically.[36] While many states similarly have limited their laws, some have expanded the scope of

31. *Id.* § 1798.82(g)(3).

32. *Id.*

33. Alabama, Kentucky, New Mexico, and South Dakota have not yet enacted data breach notification legislation. *See* National Conference of State Legislatures, State Security Breach Notification Laws, Apr. 12, 2010, http://www.ncsl.org/IssuesResearch/Telecommunications InformationTechnology/SecurityBreachNotificationLaws/tabid/13489/Default.aspx (last visited May 7, 2010); Scott Berinato, *CSO Disclosure Series*: *Data Breach Notification Laws, State by State*, CSO ONLINE, Feb. 12, 2008 http://www.csoonline.com/article/221322/CSO_Disclosure_ Series_Data_Breach_Notification_Laws_State_By_State; Personal Information Protection Act, ALASKA STAT. § 45.48.010 (West Supp. 2009); Financial Identity Fraud and Identity Theft Protection Act, S.C. CODE ANN. § 37-20-110 (Supp. 2008).

34. *See* CROWELL MORING, STATE LAWS GOVERNING SECURITY BREACH NOTIFICATION (2010), http://www.crowell.com/pdf/SecurityBreachTable.pdf; ALYSA ZELTZER HUTNIK, KELLY DRYE, STATE LAWS REQUIRING DATA BREACH NOTIFICATION (2008) (available on request from author).

35. *See* CROWELL MORING, *supra* note 34.

36. California Security Breach Information Act § 1798.82(d).

their laws to include paper records.[37] Likewise, while many state laws have adopted California's "standard" definition of personal identifying information, some states have expanded this definition to include additional information. For example, North Carolina's definition of Personal Information includes digital signatures, biometric data, fingerprints, and parents' legal surnames prior to marriage.[38] Hawaii and several other states have expanded their laws to require notification when account, credit, or debit card numbers are accessed without password or pin numbers.[39] Given these disparities, a breach could require notification under some state laws but not others.

37. Alaska, Hawaii, Indiana, Maryland, North Carolina, and Wisconsin have expanded their laws to include paper records. Personal Information Protection Act, ALASKA STAT. § 45.48.010 (West Supp. 2009); HAW. REV. STAT. ANN. § 487N-2 (LexisNexis 2009) (discussing notice of security breach); IND. CODE ANN. § 24-4.9-2-2(a) (West 2008) (discussing disclosure of a security breach); Maryland Personal Information Protection Act, M.S.C. CODE ANN., COM. LAW § 14-3504 (LexisNexis Supp. 2007) (discussing Security Breach); Identity Theft Protection Act, N.C. GEN. STAT. ANN. § 75-65 (2007); WIS. STAT. ANN. § 895.507 (2006) (Notice of Unauthorized Acquisition of Personal Information).

38. Under the law, personal information means a person's first name or first initial in combination with either (1) social security number or employer taxpayer identification number; (2) driver's license number, state identification card, or passport numbers; (3) checking account numbers; (4) savings account numbers; (5) credit card numbers; (6) debit card numbers; (7) personal identification (PIN) code; (8) electronic identification numbers, electronic mail names or addresses, internet account numbers, or internet identification names; (9) digital signatures; (10) any other numbers or information that can be used to access a person's financial resources; (11) biometric data; (12) fingerprints; (13) passwords; and (14) parent's legal surname prior to marriage. *See* N.C. GEN. STAT. ANN. § 75-66 (2007). However, personal information shall not include electronic identification numbers, electronic mail names or addresses, internet account numbers, internet identification names, parent's legal surname prior to marriage, or a password unless this information would permit access to a person's financial account or resources. *Id.* § 75-65(a).

39. HAW. REV. STAT. ANN. § 487N-1 (LexisNexis 2009). Alaska, the District of Columbia, Georgia, Illinois, Kansas, Maine, Massachusetts, Vermont, and Wisconsin all require notification if account numbers are accessed with or without passwords. ALASKA STAT. § 45.48.090 (West Supp. 2009); D.C. CODE ANN. § 28-3851(3)(A)(ii) (LexisNexis Supp. 2009); GA. CODE ANN. § 10-1-911(6) (2009); Personal Information Protection Act, 815 ILL. COMP. STAT. ANN. 530/5 (West 2008); KAN. STAT. ANN. § 50-7a01 (Supp. 2008); ME. REV. STAT. ANN. tit. 10, § 1347 (Supp. 2008); MASS. GEN. LAWS ch. 93H, § 1 (2007); VT. STAT. ANN. tit. 9, § 2430 (2007); WIS. STAT. ANN. § 895.507 (2006).

2. Exemptions

Most state data breach notification laws do not require notification of all breaches involving personal information. Instead, the laws allow for exemptions in some situations. All currently enacted state data breach laws provide an "encrypted data safe harbor"—they do not require notification of a breach if the compromised data was encrypted.[40] Almost all laws also provide exemptions for information that is publically available.[41] Additionally, many states provide a "risk of harm" exemption.[42] This exempts a company from its notification requirements if, after appropriate investigation, the company reasonably determines that a breach has not resulted or is unlikely to result in harm to the individuals whose personal information has been acquired.[43] For example, Arizona's law requires notification only if the breach "causes or is likely to cause substantial economic loss to an individual."[44] Hawaii's law requires disclosure only "where an illegal use of the personal information has occurred,

40. Despite this exemption, Alaska, Indiana, Massachusetts, Michigan, New Hampshire, New Jersey, New York, North Carolina, Oklahoma, Oregon, Pennsylvania, Virginia, and West Virginia require notification if the encryption key was also compromised in the breach. Massachusetts's law, for example defines "breach of security" as "the unauthorized acquisition or unauthorized use of unencrypted data or, encrypted electronic data and the confidential process or key that is capable of compromising the security, confidentiality, or integrity of personal information." MASS. GEN. LAWS ch. 93H, § 1 (2007). *See also* ALASKA STAT. § 45.48.090(7) (West Supp. 2009); IND. CODE ANN. § 24-4.9-2-2(b)(2) (West Supp. 2009); MICH. COMP. LAWS ANN. § 445.72(1)(b) (West Supp. 2009); N.H. REV. STAT. ANN. § 359-C:19 (200();N.J. STAT. ANN. § 56:8-161 (West Supp. 2009); N.Y. GEN. BUS. LAW § 899-aa(1)(b)(3) (McKinney Supp. 2009); N.C. GEN. STAT. ANN. § 75-66 (2007); OKLA. STAT. § 74-3113.1D(2) (2006); Oregon Consumer Identity Theft Protection Act, OR. REV. STAT. § 646.602(11) (West Supp. 2009); 73 PA. CONS. STAT. § 2303(b) (West 2008); VA. CODE ANN. § 18.2-186.6 (2009); W.VA. CODE ANN. § 46A-2A-102(b) (LexisNexis Supp. 2009).

41. *See* SCOTT & SCOTT, STATE DATA BREACH NOTIFICATION LAWS (2007), http://www.scottandscott/lp.com/resources/state_data_breach_notification_law.pdf.

42. *See* Rawitz & Frid, *supra* note 25; HUTNIK, *supra* note 34. The laws enacted by California, District of Columbia, Illinois, Minnesota, Nevada, North Dakota, Tennessee, and Texas do not include any form of this exemption. HUTNIK, *supra* note 34; *see* California Security Breach Information Act, CAL. CIV. CODE §§ 1798.29, 1798.82–.84 (West 2009); D.C. CODE ANN. § 28-3852 (LexisNexis Supp. 2009); 815 ILL. COMP. STAT. ANN. 530/10 (West 2008); MINN. STAT. Ann. § 325E.61 (West Supp. 2008); NEV. REV. STAT. ANN. § 603A.220 (West Supp. 2008); N.D. CENT. CODE. § 51-30-01 (2007); Tennessee Identity Theft Deterrence Act of 1999, TENN. CODE ANN. § 47-18-2107 (Supp. 2009); TEX. BUS. & COM. CODE ANN. § 521.053 (Vernon Supp. 2009).

43. *See* Rawitz & Frid, *supra* note 25; HUTNIK, *supra* note 34.

44. Notification of Breach of Security System, Nev. Rev. Stat. § 44-7501 (2008).

or is reasonably likely to occur, and that creates a risk of harm to a person."[45] Under Arkansas's law, "notification is not required if, after a reasonable investigation, the person or business determines that there is no reasonable likelihood of harm to consumers."[46]

Several state laws also exempt government agencies from compliance with the notification provisions. Instead of applying to "agencies" as does the California Act,[47] these laws direct their provisions toward "businesses" or "persons."[48] Because government agencies do not fall into either of these categories, a loophole is created by these laws for data breaches that occur when information is in the control of a government agency. Of the states whose data security breach laws apply to government agencies, four states specifically exempt these agencies from enforcement proceedings.[49] These states require government agencies to notify consumers, but they do not punish the agencies for non-compliance.[50] Florida's law specifically states that "administrative sanctions for failure to notify . . . shall not apply in the case of personal information in the custody of any governmental agency or subdivision."[51] These provisions seriously undermine the effectiveness of the notification laws. This loophole for government entities is especially troublesome given the large number of data breaches caused by government agencies.[52]

---

45. HAW. REV. STAT. ANN. § 487N-1 (LexisNexis 2009).

46. Personal Information Protection Act, ARK. CODE ANN. § 4-110-105(d) (Supp. 2009).

47. California Security Breach Information Act § 1798.29.

48. Connecticut, Georgia, Montana, North Dakota, Texas, and Utah's laws define breach in this way. CONN. GEN. STAT. ANN. § 36a-701b(b) (West Supp. 2009); GA. CODE ANN. § 10-1-911(2) (2009); MONT. CODE. ANN. § 30-14-1704(1) (2009); N.D. CENT. CODE. § 51-30-02 (2007); TEX. BUS. & COM. CODE ANN. § 521.053(a) (Vernon Supp. 2009); UTAH CODE ANN. § 13-33-202 (2005).

49. Florida, Hawaii, Maine, and Tennessee specifically exclude government entities from enforcement proceedings. HAW. REV. STAT. ANN. § 487N-2 (LexisNexis 2009) (excluding government agencies from actions to recover $2,500 penalties and attorneys fees); FLA. STAT. ANN. § 817.5681 (West 2006) ("[t]he administrative sanctions outlined in this section shall not apply in the case of personal information in the custody of any governmental agency or subdivision."); ME. REV. STAT. ANN. tit. 10, § 1349 (Supp. 2008) (specifying that a fine of $500 for each violation of the statute "does not apply to State Government"); TENN. CODE ANN. § 47-18-2107 (Supp. 2009).

50. *See supra* note 49.

51. FLA. STAT. ANN. § 817.5681(1)(d) (West 2006).

52. *See* Chronology of Data Breaches, *supra* note 1. In the first half of 2008, government data breaches accounted for seventeen percent of total data breaches. William Jackson, *Data Breaches up, but Not in Government Sector*, GOVERNMENT COMPUTER NEWS, July 1, 2008,

3. Notification Procedures and Timelines

Even when a company has determined that it must disclose a breach to its consumers, state laws vary as to how and when this disclosure must take place.[53] Most state statutes require that notification be made in "the most expedient time possible" and "without unreasonable delay."[54] The ambiguity of these terms may cause confusion for companies attempting to comply with breach laws in the aftermath of a breach. Florida requires that notification be made within 45 days and is the only state to provide a specific time period for notification.[55] Ohio and Wisconsin each require that notice be provided "in the most expedient time possible but not later than forty-five days."[56] Florida and Ohio's laws impose strict penalties for non-compliance with these deadlines.[57]

All of the currently enacted data breach notification laws allow for the use of substitute notification in certain cases.[58] Typically, substitute notice is permitted when the cost of providing notice exceeds $250,000 or the number of affected individuals is more than

---

http://gcn.com/Articles/2008/07/01/Data-breaches-up-but-not-in-government-sector.aspx. While this number is down from 30 percent just two years ago, government entities still represent large proportion of annual breaches. *Id.* Additionally, the Veterans Affairs government data breach remains in the top ten largest data breaches. *See* 10 Largest Breaches Since 2000, *supra* note 17.

53. *See* Rawitz & Frid, *supra* note 25; HUTNIK, *supra* note 34. Notably, however, all enacted state data breach legislation provides for a delay if the notification would impede a criminal investigation. Newer legislation puts the burden onto the law enforcement agency to request that the company delay the notification. *See* Rawitz & Frid, *supra* note 25.

54. Hutnik, *supra* note 34. While not explicitly stated in the laws, regulators in California, North Carolina, and Vermont recommend that notice be provided within ten days following discovery of the breach. *Id.*

55. FLA. STAT. ANN. § 817.5681(1)(b) (West 2006). This law has been criticized for the possibility that it may discourage businesses from providing notification earlier than the forty-five day deadline. *Id.*

56. OHIO REV. CODE ANN. § 1347.12(B)(1) (West Supp. 2009); *see* WIS. STAT. 895.507(3)(a) (2006) (notice must be made "within a reasonable time, not to exceed 45 days.").

57. In Ohio companies can be fined up to $1,000 a day for the first sixty days of non-compliance, $5,000 a day for days sixty-one through ninety, and $10,000 a day for non-compliance after the ninety-first day. *See* OHIO REV. CODE ANN. § 1349.192(A)(1) (West Supp. 2009). In Florida companies are fined $1,000 for every day up to thirty days after the forty-five day enforcement period and $50,000 for each thirty-day period or portion thereof for up to 180 days after the forty-five day notification period. FLA. STAT. ANN. § 817.5681(1)(b)(1) (West 2006).

58. *See* Rawitz & Frid, *supra* note 25; Hutnik, *supra* note 34.

500,000.[59] However, the threshold at which substitute notification is allowed has been raised or lowered by some state legislatures.[60] In addition to consumer notification, some state laws require that notice be given to consumer reporting agencies or state regulators.[61]

---

59. *See* Rawitz & Frid, *supra* note 25.

60. For example, Alaska's law states that substitute notification may be provided "if the information collector demonstrates that the cost of providing notice would exceed $150,000, that the affected class of state residents to be notified exceeds 300,000, or that the information collector does not have sufficient contact information to provide notice." ALASKA STAT. § 45.48.030(3) (West Supp. 2009). Hawaii allows substitute notification if the cost exceeds $100,000 or if the affected class to be notified exceeds 200,000. HAW. REV. STAT. ANN. § 487N-2(e)(4) (LexisNexis 2009).

61. *See* Rawitz & Frid, *supra* note 25; HUTNIK, *supra* note 34. Indiana has no numerical threshold for notification to consumer reporting agencies. *See* IND. CODE ANN. § 24-4.9-2-2(a) (West Supp. 2008). In Minnesota the threshold is 500 consumers. *See* MINN STAT. ANN. § 325E.61 subdiv. 2 (West Supp. 2008). In Alaska, Colorado, the District of Columbia, Florida, Hawaii, Kansas, Maine, Maryland, Michigan, Nevada, New Hampshire, New Jersey, North Carolina, Ohio, Oregon, Pennsylvania, South Carolina, Tennessee, Vermont, Virginia, and West Virginia, notice must be provided to credit reporting agencies if more than 1,000 consumers are notified. ALASKA STAT. § 45.48.040(a) (West Supp. 2009); COLO. REV. STAT. ANN. § 6-1-716(2)(d) (West Supp. 2009); D.C. CODE § 28-3851(C) (LexisNexis Supp. 2009); FLA. STAT. ANN. § 817.5681(12) (West 2006); HAW. REV. STAT. ANN. § 487N-2(f) (LexisNexis 2009); KAN. STAT. ANN. § 50-7a02(f) (Supp. 2008); ME. REV. STAT. ANN. tit. 10, § 1348(4) (Supp. 2008); MD. CODE ANN., COM. LAW § 14-3506(a) (LexisNexis Supp. 2008); MICH. COMP. LAWS ANN. § 445.72(8)(a) (West Supp. 2009); NEV. REV. STAT. ANN. § 603A.220(6) (West Supp. 2009); N.H. REV. STAT. ANN. § 359-C20(VI)(a) (2009); N.J. STAT. ANN. § 56:8-163(f) (West Supp. 2009); N.C. GEN. STAT. ANN. § 75-65(f) (2007); OHIO REV. CODE ANN. § 1349.19(G) (West Supp. 2009); OR. REV. STAT. ANN. § 646.604(6) (West Supp. 2009); 73 PA. CONS. STAT. ANN. § 2305 (West 2008); S.C. CODE ANN. § 1-11-490(I) (2008); TENN. CODE ANN. § 47-18-2107(g) (Supp. 2009); VT. STAT. ANN. tit. 9, § 2435(c) (2006); VA. CODE ANN. § 18.2-186.6(E) (2009); W.VA. CODE ANN. § 46A-2A-102(f) (LexisNexis Supp. 2009). In New York, the threshold is 5,000. *See* N.Y. GEN. BUS. LAW § 899-aa(8)(b) (McKinney Supp. 2009). Georgia and Texas have thresholds of 10,000. *See* GA. CODE ANN. § 10-1-912(d) (2009); TEX. BUS. & COM. CODE ANN. § 521.053(h) (Vernon Supp. 2009). Montana requires CRA notice only if the notice to consumers mentions credit reports. *See* MONT. CODE ANN. § 30-14-1704(7) (2009). Massachusetts requires CRA notice to CRA's identified by the Director of Consumer affairs. *See* MASS. GEN. LAWS ch. 93H, § 3(b)(2) (2007).

Maine, Maryland, Massachusetts, New Hampshire, New Jersey, New York, and Virginia have no numerical threshold for regulator notification (although in New Jersey and Maryland the notice must be sent before the consumer notice). *See* ME. REV. STAT. ANN. tit. 10, § 1348 (Supp. 2008); MD. CODE ANN., COM. LAW § 14-3504 (LexisNexis Supp. 2008); MASS. GEN. LAWS ch. 93H, § 1 (2007); N.H. REV. STAT. ANN. § 359-C:20 (2009); N.J. STAT. ANN. § 56:8-163 (West Supp. 2009); N.Y. GEN. BUS. LAW § 899aa (McKinney Supp. 2009); VA. CODE ANN. § 18.2-186.6(B) (2009). In Hawaii, North Carolina, and South Carolina, the threshold for notification is more than 1,000. *See* HAW. REV. STAT. ANN. § 487N-2 (LexisNexis 2009); N.C. GEN. STAT. ANN. § 75-65 (2007); S.C. CODE ANN. § 37-20-110 (Supp. 2008). Under Vermont's law, notification to the Vermont Attorney General must be provided only if an investigation

4. Enforcement

The existing state data breach notification laws also vary as to who has a cause of action following a violation of the law.[62] Some of the laws allow for a private right of action, while others do not.[63] In practice, due to the difficulty of proving actual damages in many data breach and failure-to-notify cases, this private right of action may be of limited value to consumers.[64]

### *D. Other measures*

In addition to data breach notification laws, several states have enacted legislation in recent years that requires companies to protect consumer data prior to a breach. For example, several states[65] have enacted laws that require businesses to implement and maintain

---

reveals that misuse of the breached personal information is not reasonably possible. *See* VT. STAT. ANN. tit. 9, § 2435 (2006).

62. *See* HUTNIK, *supra* note 34.

63. *Id.* California, the District of Columbia, New Hampshire, North Carolina, Oregon, South Carolina, Tennessee, and Washington currently allow for a private right of action by consumers who have been affected by a data breach. California Security Breach Information Act, CAL. CIV. CODE § 1798.84 (West 2009); D.C. CODE ANN. § 28-3853(a) (LexisNexis Supp. 2009); N.H. REV. STAT. ANN. § 359-C:21(I) (2009); N.C. GEN. STAT. ANN. § 75-65 (2007); OR. REV. STAT. ANN. § 646A.624 (West Supp. 2009); S.C. CODE ANN. § 37-20-170 (Supp. 2008); TENN. CODE ANN. § 47-18-2107(h) (Supp. 2009); WASH. REV. CODE ANN. § 19.255.010(10)(9) (West 2007).

64. *See* Gregory T. Parks & Megan E. Adams, *Can Your Firm Be Sued for a Data Breach?*, E-COMMERCE TIMES, Dec. 8, 2006, http://www.ecommercetimes.com/story/54620.html.

> Data security breaches often do not cause any identifiable or quantifiable harm to the individuals whose information was compromised. In certain cases, courts have therefore labeled the damages claimed by plaintiffs as "speculative" or "nonexistent" and have dismissed lawsuits because of this defect. However, certain political and legislative developments indicate that the climate could soon change.

*Id.*

65. Arkansas, California, Maryland, Nevada, North Carolina, Oregon, Rhode Island, Texas, and Utah each have enacted such a law. Personal Information Protection Act, ARK. CODE ANN. § 4-110-104 (Supp. 2009); California Security Breach Information Act § 1798.81.5; MD. CODE ANN., COM. LAW § 14-3503(a) (LexisNexis Supp. 2008); NEV. REV. STAT. ANN. § 597.970 (West Supp. 2009); N.C. GEN. STAT. ANN. § 75-64 (2007); OR. REV. STAT. ANN. § 646A.622 (West Supp. 2009); Identity Theft Protection Act, R.I. GEN. LAWS § 11-49.2-2(2) (Supp. 2008); TEX. BUS. & COM. CODE ANN. § 521.052 (Vernon Supp. 2009); Protection of Personal Information Act, UTAH CODE ANN. § 13-44-201 (Supp. 2009).

reasonable security measures to protect personal information from "unauthorized access, destruction, use, modification, or disclosure."[66] In addition to these information safeguard laws, at least nineteen states have enacted laws that regulate how businesses dispose of records containing personal data.[67] Additionally, many states have adopted laws requiring businesses to protect Social Security numbers from public access.[68]

---

66. *See* Alysa Zeltzer Hutnik, *State Privacy and Data Protection Laws: Let's Recap*, PRIVACY TRACKER, Mar. 2008, at 5 (on file with author).

> There are, however, some variances among these laws. The Oregon safeguard law identifies specific administrative, technical, and physical safeguards as examples of the measures necessary to demonstrate compliance with the law. The Texas safeguard law further specifies that the obligation to implement and maintain reasonable safeguard procedures includes taking any appropriate corrective action. The Nevada law also expressly requires businesses to encrypt certain personal information if transferring that information electronically outside of the security business network. The California law also prohibits businesses form recording personal information on transaction records. And about half of the laws expressly require . . . the third parties to protect the personal information to the same extent that the business must protect that information, by contract. Finally, the North Carolina law is limited to licensed insurers, and the Oregon, Texas, and Utah safeguard laws contain an exemption for financial institutions.

*Id.* at 6.

67. *Id.* Arkansas, California, Georgia, Hawaii, Indiana, Kentucky, Maryland, Massachusetts, Michigan (applies only to health care providers), Montana, Nevada, New Jersey, New York, Oregon, Tennessee, Texas, Utah, Vermont, Washington, and Wisconsin (financial institutions, medical business, and tax preparation business only). *Id.*; *see* ARK. CODE ANN. § 4-110-104, *supra* note 64; CAL. CIV. CODE § 1798.81; GA. CODE ANN. § 10-15-2 (2009); HAW. REV. STAT. ANN. § 487R-2 (LexisNexis 2009); IND. CODE ANN. § 28-1-2-30.5(h) (West Supp. 2008); KY. REV. STAT. ANN. § 365.725 (LexisNexis 2008); MD. CODE ANN., COM. LAW § 14-3502(b); MICH. COMP. LAWS ANN. § 445.72a (West Supp. 2009); MONT. CODE. ANN. § 30-14-1703 (2009); NEV. REV. STAT. ANN. § 603A.200 (West Supp. 2009); N.Y. GEN. BUS. LAW § 899-aaa (McKinney Supp. 2009); OR. REV. STAT. ANN. § 646A.622; TEX. BUS. & COM. CODE ANN. § 521.052(b) (Vernon Supp. 2009); UTAH CODE ANN. § 13-44-201 (Supp. 2009). These laws require that when businesses dispose of consumer records containing personal information, they destroy the records by shredding, erasing, or otherwise modifying the records to make them unreadable or undecipherable. Some of these laws exempt certain industries that already have been heavily regulated by federal or state law. *Id.*

68. Only Alabama, Alaska, Idaho, Iowa, Kentucky, Massachusetts, Nebraska, New Hampshire, Ohio, Pennsylvania, Tennessee, West Virginia, and Wyoming have failed to enact legislation specifically protecting Social Security Numbers. *See* Federal Trade Commission, State Laws: Social Security Numbers, http://www.ftc.gov/bcp/edu/microsites/idtheft/law-enforcement/state-laws-social-security.html (last visited May 7, 2010). Generally, these laws prohibit business from publically posting or displaying a Social Security number, requiring consumers to transmit a SSN over the internet unless the connection is secure or the number is encrypted, requiring consumers to log onto a website using a SSN without a password, printing

Minnesota has enacted the "Plastic Card Security Act," which codifies the core requirements of a standard developed by the Payment Card industry.[69] The law is designed to motivate businesses to protect financial cardholder data by transferring the cost of breaches caused by payment card processing from financial institutions to retailers.[70] The law prohibits businesses from retaining card security code data, pin verification code numbers, or any magnetic stripe data for more than 48 hours after a card transaction has been approved.[71] A business that violates these requirements may be required to reimburse card issuers for the reasonable costs undertaken to respond to a breach.[72]

### *E. Previously Proposed Federal Legislation*

While no federal data breach notification legislation has yet been enacted, numerous bills have been introduced in Congress to address security breaches.[73] Many of these proposed laws resemble those

---

SSNs on identification card or badges, or printing SSNs on anything mailed to a consumer unless required by law or the document is a form or application. *Id.* In New Jersey and New York, these measures have been expanded to apply to truncated SSNs as well. *Id. See also* Hutnik, *State Privacy and Data Protection Laws*, *supra* note 66.

69. Plastic Card Security Act, MINN. STAT. ANN. § 325E.64 (West Supp. 2008). *See* Payment Card Security Laws Create New Costs for Retailers, http://www.adlawbyrequest legacy.com/legislation.cfm?cit_id=2779&FaArea2=CustomWidgets.content_view1&usecache= false&ocl_id=ARTICLE (June 29, 2007). The Payment Card Industry Association is:

> . . . a group comprised of the major card issuers along with some larger merchants such as Wal-Mart. PCIA created the PCI Data Security Standard and the Data Security Audit Guidelines in an attempt to develop a self-regulatory solution to identify theft and data security compromises.
>
> In addition to complying with the standard and guidelines themselves, PCIA members must contractually obligate everyone in the chain of payment card transactions to abide by the requirements. . . .
>
> . . . [S]everal states, at the urging of financial institutions have begun to incorporate elements of the PCI standard into legislation.

*Id.*

70. *See* Hutnik, *State Privacy and Data Protection Laws*, *supra* note 66.

71. *See* Plastic Card Security Act § 325E.64, subdiv. 2.

72. *Id.* § 325E.64, subdiv. 3. These costs include the costs of canceling and reissuing credit and debit cards, closing and reopening accounts, stop-payment actions, unauthorized transaction reimbursements, and the providing of breach notification to account holders. *Id.*

73. *See* GINA MARIE STEVENS, CRS REPORT FOR CONGRESS, DATA SECURITY: FEDERAL LEGISLATIVE APPROACHES (2006), *available at* http://www.policyarchive.org/handle/10207/

passed by the states.[74] However, some of the more recently proposed federal laws have suggested sweeping new reforms for data notification policy.[75]

Of the many data breach notification laws proposed in the 110th Congress, four are especially noteworthy.[76] S.239, the Notification of Risk to Personal Data Act, was introduced by Senator Feinstein (D-CA).[77] H.R. 958, the Data Accountability and Trust Act, was introduced by Rep. Rush (D-NJ).[78] H.R. 836, the Cyber-Security Enhancement and Consumer Data Protection Act of 2007, was introduced by Rep. Smith (D-Wash).[79] S.B. 495, the Personal Data Privacy and Security Act of 2007, was introduced by Senator Leahy (D-VT).[80] Each of these bills would preempt state data breach notification laws.[81] Additionally, all four bills explicitly state that they do not provide a private right of action.[82] S. 239, H.R. 958, and

---

2745 (providing an overview of data breach notification laws proposed in the first session of the 109th Congress).

74. *Id. See also* Scott Berinato, *CSO Disclosure Series: What's Next With Disclosure Legislation?*, CSO ONLINE, Feb. 11, 2008, http://www.csoonline.com/article/217027/CSO_Disclosure_Series_What_s_Next_with_Disclosure_Legislation_?page=? (explaining that most proposed bills are meant to copy what the states have already done).

75. *See* Anne Broache, *Data Breach Bills Resurface in Congress*, CNET NEWS, Feb. 6, 2007, http://news.cnet.com/2100-7348-6156904.html. For example, The Cybersecurity Enhancement and Consumer Data Protection Act, proposed by Rep. Lamar Smith, would make it a crime punishable by up to five years in prison to withhold information about a major security breach from the FBI and the U.S. Secret Service. *Id.* The bill would require stewards of information that experience a breach to notify those investigative services within fourteen days of discovering it. Failure to do so would result in fines of up to $50,000 a day. *Id. See also* Cybersecurity Enhancement and Consumer Data Protection Act of 2007, H.R. 836, 110th Cong. (2007).

76. *See* Posting of Clifford Davidson to Proskauer Rose Privacy Law Blog, http://privacylaw.proskauer.com/2007/03/articles/security-breach-notification-laws/110th-congress-proposes-sweeping-federal-data-security-legislation/ (Mar. 6, 2007); Berinato, *CSO Disclosure Series: What's Next With Disclosure Legislation?*, *supra* note 74.

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

78. Data Accountability and Trust Act, H.R. 958, 110th Cong. (2007).

79. H.R. 836, 110th Congress, *supra* note 95.

80. Personal Data Privacy and Security Act of 2007, S. 495, 110th Cong. (2007).

81. Preemption has been the source of debate between business and privacy group advocates. Industry groups advocate for a narrow federal law that would preempt all differing state laws in order to streamline the notification process for affected companies. Privacy advocates favor a national law that would allow states to enact stronger laws in order to ensure that consumers obtain the strongest protections possible. *See* STEVENS, *supra* note 73.

82. None of the currently pending federal data breach notification laws allow for a private right of action. Under these laws, only state attorneys general could sue for violation of statutes.

S. 458 would allow the Federal Trade Commission to establish guidelines for data security and breach notification.[83] S. 495 and H.R. 958 set forth data security requirements in addition to data breach notification guidelines.[84] H.R. 836 would criminalize the concealment of a data breach.[85] Through these and other data breach notification bills, Congress has made clear that data security legislation is a top priority.[86]

## II. ANALYSIS

### *A. Critique of State Data Breach Notification Laws*

While the current state data breach notification laws provide consumers with valuable information regarding the security of their personal information, these laws are far from perfect and for several reasons do not sufficiently address the problems created for both consumers and businesses by data breaches. First, the laws are primarily reactive. As a result, the laws have only a limited chance of preventing breaches. Second, the ambiguous requirements created by the large patchwork of disparate state laws make corporate compliance following a breach difficult and costly. Third, the current system of regulation has left many loopholes in coverage. As a result, many consumers may be left un-notified if their data is compromised.

---

*See* Berinato, *supra* note 74; Davidson, *supra* note 76.

83. Davidson, *supra* note 76.

> Although the FTC's mandate has until now not included breach notification, the FTC has a fair amount of experience with enforcing data security standards under its Section 5 authority. The proposed legislation delegates authority to the FTC to promulgate regulations based on criteria similar to those the FTC already follows in its FTC cases: establishment of security policies, enforcement of those policies and monitoring of potentially vulnerable systems.

*Id.*

84. *See* Data Accessibility and Trust Act, H.R. 958, 110th Cong. (2007); Personal Data Privacy and Security Act of 2007, S. 495 110th Cong. (2007); Davidson, *supra* note 76.

85. *See* Cybersecurity Enhancement and Consumer Data Protection Act of 2007, H.R. 836, 110th Cong. (2007); Broache, *supra* note 75.

86. *See* Broache, *supra* note 75 ("the senator [Leahy] listed passage of new data breach security laws among his top priorities."); Berinato, *CSO Disclosure Series: What's Next With Disclosure Legislation?*, *supra* note 74; Davidson, *supra* note 76 ("Congressional leaders have emphasized that data privacy and breach notification are top priorities.").

1. Reactive v. Proactive

One of the primary flaws in state data breach notification laws is that they require notification only after a breach has occurred, while virtually ignoring breach prevention.[87] By imposing liability on companies for failing to notify consumers following a breach, rather than for failing to prevent the breach itself, the laws as they currently stand do not adequately incentivize companies to protect consumer data.[88] Instead, they merely require companies to master the notification system created by the state laws. The notification requirement itself may motivate some companies to safeguard consumer information in order to avoid the bad publicity surrounding a large data breach. However, the large number of data breaches revealed in the years following the enactment of California's Security Breach Information Act is a testament to the ineffectiveness of these laws as a means of adequately preventing data breaches.[89] As detailed above, some states have taken proactive measures to ensure that consumer data is protected from a breach.[90] While these measures are a step in the right direction, a federal law is needed to impose these preventative measures uniformly.

2. Ambiguity

The current system of state data breach notification laws imposes specific obligations on a company following a data breach; however, given the vast disparities among current state laws, these obligations are not clearly defined.[91] In the time immediately following a breach,

87. *See* California Security Breach Information Act, CAL. CIV. CODE § 1798.82, hist.n.1(R) (stating that the reason for enacting the legislation is to provide "expeditious notification" of security breaches so that victims of identity theft can act quickly to minimize any damage). While the legislators may also have intended the act to lower the number of reported data breaches, this goal is not explicitly stated in the Act. *Id.*

88. *See* Robert Westervelt, *Industry Group Uses Awareness Month to Lobby for Data Breach Laws*, SEARCHSECURITY, Oct. 8, 2007, http://searchsecurity.techtarget.com/news/article/0,289142,sid14_gci1275883,00.html.

89. *See* Chronology of Data Breaches, *supra* note 1.

90. *Infra* Part D.

91. *See* Brett Lockwood, *When the Dam Breaks: Compliance with Data Breach Notification and Data Privacy Laws*, TAG, July 10, 2008, http://www.tagonline.org/articles.

the variations among the laws create challenges for business management personnel in determining with which, if any, of the forty-four data breach notification laws they must comply.[92] Because many modern companies maintain records for consumers from more than one state, a breach often triggers several, if not all, of the currently enacted laws.[93] While these laws are rarely in direct conflict, they do differ in regard to applicability; exemptions; notification procedures and timelines; and enforcement.[94] This can create unnecessary confusion and cost that could be avoided by the enactment of a federal data breach notification law providing clear guidelines for businesses following a breach.[95]

3. Loopholes/Exemptions

Perhaps the most critical problem with current state data breach notification laws is that the patchwork system created by the state laws does not cover everyone. The forty-five state laws each require companies to provide notification only to consumers residing within the state. This means that residents of the five states that have yet to enact legislation may not receive notification if their information is compromised. Furthermore, several of the current laws create

---

php?id=286 (noting that "[c]ompliance with data privacy laws continues to bedevil executive management" due to the variances in the laws).

92. *See id.*

93. *See* Philip Alexander, *Data Breach Notification Laws: A State-By-State Perspective*, INTELLIGENT ENTERPRISE, Apr. 9, 2007, http://www.intelligententerprise.com/showArticle.jhtml?articleID=198800638. For the many companies conducting business online, compliance can be especially difficult. Online sales may trigger obligations under all forty-two current data breach notification laws.

94. *See* Lockwood, *supra* note 91.

95. *Id.*

> In light of the divergent state laws dealing with notification of data breaches and the related compliance burden, many business groups reluctantly have championed legislation at the federal level to bring uniformity to this area. . . . Among the many reasons that none of the widely discussed bills has been passed thus far has been the inability to reconcile the inherent competing interests between consumer groups, who want to have federal requirements layered onto co-existing state requirements, and the demands of the business community for a single federal regime that would preempt state laws and possibly relax some of the more stringent state requirements, such as those imposed by California.

*Id.*

exemptions for government entities.[96] Recent years have shown that these agencies are not immune from data breaches.[97] In fact, these entities suffer from some of the most frequent and largest data breaches.[98] A federal law is necessary to ensure that universal coverage is provided and that consumers are notified every time their personal information is compromised.

## III. PROPOSAL

The current state data breach notification system is ambiguous and difficult for companies to navigate following a breach and has created loopholes that have left many consumers unprotected. Additionally, the current laws work primarily to regulate responses following a breach, doing little to address the issue of data breach prevention. Congress should take action immediately to enact a federal data breach notification law. In addition to establishing standardized notification requirements, this law should require companies to take preventive steps to avoid data breaches and impose liability on those companies that fail to do so.

A successful data breach notification law should combine elements of both existing state data breach notification laws and previously proposed federal notification laws. First, federal data breach notification legislation must provide standardization. Replacing the current patchwork of 45 state laws with a single comprehensive federal law would give businesses a clear road map to follow after a breach. This law would eliminate questions regarding what information is covered and when and how notification must be provided, and would preempt all state data breach notification laws. Second, a federal data breach law must cover everyone. Any law that

---

96. *See* Alexander, *supra* note 93.

> It's important to know your customer base and in which states they reside. . . . Be carefully [sic] when considering selective breach disclosures based solely on a lack of legal requirements to notify customers in certain states. The public relations fall-out could be more damaging to your company than the actual disclosure itself.

*Id.* In many large breaches, companies will notify all affected consumers despite the lack of a technical legal obligation to do so. *See supra* note 7 and accompanying text.

97. *See* Chronology of Data Breaches, *supra* note 1.

98. *See supra* note 52 and accompanying text.

excludes government entities ignores the reality that consumer information is at risk of disclosure from the public as well as the private sector. Third, a federal law must provide support to affected consumers in the form of credit monitoring. This provision would help notified consumers take action to prevent identity theft. Fourth, a law should have a "risk of harm" exception. Under this exception, a company would be able to forgo notification of a breach that presented no reasonable harm to consumers. This exception would help prevent consumers from receiving an influx of useless notifications. Fifth, the law should require notification of each breach to consumer reporting agencies and create an FTC clearinghouse. This centralized clearinghouse would allow for collection of accurate national data breach statistics. Sixth, both the FTC and state Attorneys General should be given power to enforce the new federal law. Consumers should also be afforded a private right of action. Seventh, companies should be held liable not only for failure to notify, but also if they negligently allow a data breach to occur. This would give companies greater motivation to protect consumer data and prevent data breaches. Eighth, the law should establish data protection and disposal requirements that would help to prevent data breaches. Ninth, the law should require companies to establish policies that would allow them to react quickly if a data breach occurs.[99]

## CONCLUSION

In the years since the ChoicePoint data breach first brought widespread attention to the issue of data breach notification, data breaches have remained an important concern for both consumers and companies. The forty-five existing state data breach notification laws provide some protection by requiring notification to affected consumers following a breach. However, this patchwork of laws has resulted in an ambiguous notification system that is challenging for companies to navigate. The system also fails to provide notification to all affected consumers due to loopholes created by the laws and the

99. Government entities are required to establish such policies under the guidance set forth by the OMB. *See* OFFICE OF MGMT. & BUDGET, *supra* note 21.

failure of some states to enact legislation. This ambiguity has created the need for a federal law to provide clear, uniform guidelines for data breach notification. Unlike the current state laws, which generally are reactive, this federal law should take proactive steps to prevent breaches before they occur.