St. John's Law Review

Volume 84
Number 4 *Volume 84, Fall 2010, Number 4*

Article 8

A Simple Compromise: The Need for a Federal Data Breach Notification Law

Jacqueline May Tom

A SIMPLE COMPROMISE: THE NEED FOR A FEDERAL DATA BREACH NOTIFICATION LAW

JACQUELINE MAY TOM[†]

INTRODUCTION

In 2005, the credit information of approximately 163,000 consumers was stolen from ChoicePoint, now a division of LexisNexis.[1] ChoicePoint sold the information to identity thieves impersonating business people.[2] The thieves opened ChoicePoint accounts by posing as debt collectors and insurance agents, giving them access to a large database with records on almost every individual in the United States.[3] In response, the company sent out notification letters, informing consumers that their personal information may have been compromised.[4] Ultimately,

---

[†] Senior Articles Editor, *St. John's Law Review*; J.D. Candidate, 2011, St. John's University School of Law; B.A., 2006, Boston University.

[1] Christopher Danzig, Mary Swanton & Lauren Williamson, *Breach Patrol*, INSIDE COUNSEL, May 2009, at 60.

[2] *Id.*

[3] Robert O'Harrow, Jr., *ID Data Conned from Firm:* ChoicePoint *Case Points to Huge Fraud*, WASH. POST, Feb. 17, 2005, at E01.

[4] The following is an excerpt from one of the letters:

> I'm writing to inform you of a recent crime committed against ChoicePoint that MAY have resulted in your name, address, and Social Security number being viewed by businesses that are not allowed access to such information. We have reason to believe your personal information may have been obtained by unauthorized third parties, and we deeply regret any inconvenience this event may cause you.
>
> . . . .
>
> We believe that several individuals, posing as legitimate business customers, recently committed fraud by claiming to have a lawful purpose for accessing information about individuals, when in fact, they did not. When the fraud was discovered, access to information was discontinued and the authorities were notified.
>
> . . . .
>
> We have set up a toll free number to accept calls from our customers with questions and to provide any additional advice and support we can. To speak to someone about the information in this letter, please call 1-877-[number redacted] between the hours of 6 a.m. and 7:30 p.m. Pacific time,

more than 800 cases of identity theft were connected to the incident, leading ChoicePoint to agree to a $15,000,000 settlement.[5] Since 2005, many states have enacted data breach notification laws covering when and how businesses that license, own, or maintain computerized data must notify individuals whose personal information has been breached. To date, forty-six states, the District of Columbia, Puerto Rico, and the Virgin Islands have enacted data breach notification laws.[6] Only four states—Alabama, Kentucky, New Mexico, and South Dakota—do not have a data breach notification law.[7]

Because many states have different notification requirements, businesses involved in interstate commerce and their in-house counsel are faced with a compliance nightmare. They must constantly keep abreast of any amendments to state laws that will affect their current practices and policies. This is an extremely difficult task given that data breach notification laws vary from state to state. Variations are so numerous that it is virtually impossible to convert these state laws into the more manageable format of fifty-state surveys.[8] Some surveys oversimplify the law, ignoring subtle differences,[9] while others are too detailed for practical use.[10] In most cases, looking up each of the forty-five statutes one by one is the only way to fully understand the differences. Such diligence requires a lot of time and effort.

> Monday through Friday. We hope this information is helpful to you and regret any inconvenience this may cause you.
>
> Sincerely,
>
> J. Michael De Janes, Chief Privacy Officer

ChoicePoint's Letter to Consumers Whose Information Was Compromised, CSO ONLINE, http://www.csoonline.com/article/221489/ChoicePoint-s-Letter-to-Consumers-Whose-Information-Was-Compromised (last visited Feb. 5, 2011).

[5] Danzig et al., *supra* note 1, at 60–61.

[6] A list of the statutes and links to them can be found on the National Conference of State Legislatures website, which periodically updates its list as new statutes are passed. *Security Breach Legislation 2010*, NAT'L CONFERENCE ON STATE LEGISLATURES, http://www.ncsl.org/default.aspx?tabid=20100 (last updated Oct. 12, 2010).

[7] *See id.*

[8] *See infra* Part I.

[9] *See, e.g.*, SCOTT & SCOTT LLP, STATE DATA BREACH NOTIFICATION LAWS (Sept. 21, 2007), *available at* http://www.scottandscottllp.com/resources/state_data_breach_notification_law.pdf (breaking down each state's law into six factors).

[10] *See, e.g.*, PERKINS COIE, SECURITY BREACH NOTIFICATION CHART (June 24, 2008), *available at* http://www.digestiblelaw.com/files/upload/securitybreach.pdf (describing the major elements of each state's law).

Once businesses understand the law, they must then decide how to notify affected consumers. This decision is difficult. Businesses that decide to comply with the law will find that in certain situations, some states require notification, while others do not. One option is to send one form letter complying with all the state statutes. If a business sends this form letter to every consumer who may have been affected, it could reduce its costs in the short-term. But this method could also lead to increased reputational harm because the business is choosing to notify more individuals than required by state law. Many of these individuals, having lost confidence in the particular business, may decide to take their business elsewhere. A second option is to send letters only to consumers residing in those states requiring notification. Assuming that a business knows where each of its customers resides, this option also reduces costs. However, it treats consumers from different states unequally and may be perceived as unfair. A third option is to send out personalized letters. This option is the most costly, but may preserve the most customer loyalty. Choosing between these three options requires a thorough assessment of the severity of the breach, the tenor of current customer opinion, and the costs of sending notification. Businesses that decide not to comply with the law are usually given a much simpler choice than their law-abiding counterparts. Most decide that preserving their reputation is more important than complying with the law; thus, they never notify affected consumers.[11] This is especially alarming in cases where it is difficult to trace the breach back to the records of a particular business.[12] In such cases, it is impossible to hold the business liable, so consumers remain unaware that their identities are at risk.

The fact that a federal law would simplify matters has not gone unnoticed. The 109th Congress was extremely active in trying to get a federal law passed. "At the close of 2005, there were at least seven House and Senate committees working on

---

[11] This phenomenon is referred to in one paper as the "disclosure disincentive." Edward J. Janger & Paul M. Schwartz, *Anonymous Disclosure of Security Breaches: Mitigating Harm and Facilitating Coordinated Response*, *in* SECURING PRIVACY IN THE INTERNET AGE 223, 234 (Anupam Chander et al. eds., 2008). According to this theory, businesses will decide not to disclose in two instances. *Id.* The first is when they do not want to harm their reputation, and the second is when it is impossible to trace the breach back to them. *Id.*

[12] *See id.*

federal legislation directly addressing what organizations should do when individuals' personal and private data has been illegally accessed."[13] However, "all of the bills were mired down in committees by turf wars and intense lobbying."[14] None became law. The 110th Congress took steps to pass a bill, but it, too, was unable to succeed.[15] There was also activity in the 111th Congress. Among the bills circulating were the Data Breach Notification Act (S. 139),[16] the Personal Data Security and Privacy Act (S. 1490),[17] the Data Security Act of 2010 (S. 3579),[18] the Data Security and Breach Notification Act of 2010 (S. 3742),[19] and the Data Accountability and Trust Act (H.R. 2221).[20] S. 139, S. 1490, and H.R. 2221 were all approved by their respective committees in the House and Senate. The House passed H.R. 2221 in December 2009. S. 3579 and S. 3742 were introduced most recently in the summer of 2010. None of these bills became law.

Despite all this congressional activity, whether the 112th Congress will pass a federal data breach notification law remains uncertain. Similar bills will likely face the same obstacles from lobbyists as their predecessors in previous sessions. Consumer

---

[13] Samuel Lee, Note, *Breach Notification Laws: Notification Requirements and Data Safeguarding Now Apply to Everyone, Including Entrepreneurs*, 1 ENTREPRENEURIAL BUS. L.J. 125, 136 (2006) (citing Personal Data Privacy and Security Act of 2005, S. 1789 109th Cong. (2005); Identity Theft Protection Act, S. 1408, 109th Cong. (2005); Notification of Risk to Personal Data Act, S. 1326, 109th Cong. (2005); Data Accountability and Trust Act, H.R. 4127, 109th Cong. (2005); Information Protection and Security Act, S. 500, 109th Cong. (2005); Information Protection and Security Act, H.R. 1080, 109th Cong. (2005); Financial Data Protection Act of 2005, H.R. 3997, 109th Cong.; Consumer Data Notification and Security Act of 2005, H.R. 3140, 109th Cong).

[14] Sarah Ludington, *Reining in the Data Traders: A Tort for the Misuse of Personal Information*, 66 MD. L. REV. 140, 157 (2006).

[15] *See, e.g.*, Personal Data Privacy and Security Act of 2007, S. 495, 110th Cong.; Notification of Risk to Personal Data Act of 2007, S. 239, 110th Cong.; Data Accountability and Trust Act, H.R. 958, 110th Cong. (2007); Cyber-Security Enhancement and Consumer Protection Act of 2007, H.R. 836, 110th Cong.

[16] Data Breach Notification Act, S. 139, 111th Cong. (2009).

[17] Personal Data Privacy and Security Act, S. 1490, 111th Cong. (2009).

[18] Data Security Act of 2010, S. 3579, 111th Cong.

[19] Data Security and Breach Notification Act of 2010, S. 3742, 111th Cong.

[20] Data Accountability and Trust Act, H.R. 2221, 111th Cong. (2009). Another recently proposed bill, Building Effective Strategies To Promote Responsibility Accountability Choice Transparency Innovation Consumer Expectations and Safeguards Act, not discussed in this Note, is very different from the bills already mentioned, explicitly refusing to preempt state data breach notification laws. H.R. 5777, 111th Cong. § 605(c) (2010).

protection groups and their opponents do not show signs of backing down.[21] Before taking office in 2009, President Barack Obama and his transition team attempted to restrict lobbyists in Washington, D.C.[22] Even so, lobbyists' influence remains strong.[23] In 2009, the financial services industry alone spent over $220 million on lobbying efforts.[24] Between November 2008 and March 2009, "more than 2,000 cities, companies, and associations . . . hired lobbyists to help them push their agendas on Capitol Hill and at the White House, easily outpacing such numbers after the previous two elections."[25] Thus, lobbyists' potential impact on a federal data breach notification law cannot be ignored.

While the debate among industry lobbyists rages on, security breaches continue to take place. Cybercriminals are adapting to the changing market for stolen data, targeting not only people's most vulnerable data but also their most valuable.[26] According to the Privacy Rights Clearinghouse, a nonprofit consumer information and advocacy organization, a total of 511,468,368

---

[21] *See* Letter from Ctr. for Digital Democracy et al. to Energy & Commerce Comm. Member (Sept. 29, 2009) [hereinafter Letter on H.R. 2221], *available at* http://www.privacylives.com/wp-content/uploads/2009/09/hr2221preemption29sept09.pdf (letter from various consumer protection groups); Letter from Am. Ass'n of Adver. Agencies et al. to Patrick Leahy, Chairman, Sen. Judiciary Comm. & Jeff Sessions, Ranking Member, Sen. Judiciary Comm. (Nov. 4, 2009) [hereinafter Letter on S. 1490], *available at* http://www.uschamber.com/issues/letters/2009/letter-s-1490-personal-data-privacy-and-security-act-2009 (letter from various business groups on the Personal Data Privacy and Security Act of 2009, S. 1490).

[22] For example, President Obama's transition team prohibited registered lobbyists who had lobbied during the previous twelve months from working in the policy areas on which they lobbied. *See* Helene Cooper & Jeff Zeleny, *Obama's Transition Team Restricts Help of Lobbyists*, N.Y. TIMES, Nov. 12, 2008, at A19.

[23] *See* Stephen Labaton, *Lobbyists Mass to Try To Shape Financial Reform*, N.Y. TIMES, Oct. 15, 2009, at B1 ("Even though President Obama vowed to change the culture of corporate influence on Washington, the administration has contributed, albeit inadvertently, to making this a banner year for lobbyists.").

[24] *See id.*

[25] Ellen Nakashima & Brady Dennis, *In a Down Time Everywhere Else, K Street Bustles; Lobbyists Find Plenty of Work as Clients Contend for Stimulus Package's Billions*, WASH. POST, Mar. 30, 2009, at A12.

[26] *See* WADE H. BAKER ET AL., VERIZON BUSINESS, 2009 DATA BREACH INVESTIGATIONS REPORT 5 (2009), http://www.verizonbusiness.com/resources/security/reports/2009_databreach_rp.pdf. In 2009, it seems that the most sought after data were Personal Identification Numbers ("PIN") information. *See id.*

records in the United States were compromised between 2005 and January 2011.[27] Even the President of the United States has been a victim.[28]

Clearly, it is time for legislators in Congress to reach a compromise. This Note argues that a strict federal data breach notification law would not only appease businesses tired of having to comply with forty-six different state laws but would also increase incentives for businesses to disclose by reducing the cost of compliance and increasing the reputational risk associated with security breaches. Part I of this Note examines the current state of the law by exploring the elements of a data breach notification law. This Part will compare various state laws to the bills considered by the 111th Congress. Part II analyzes lobbyists' differing perspectives on the possibility of a federal data breach notification law that preempts the state laws currently in place. Taking into account all of these perspectives, Part III draws conclusions regarding the form a federal data breach notification law should take and focuses on giving consumers increased control over the security of their own personal data.

I. THE CURRENT STATE OF THE LAW

A. The Legal Landscape

In 2003, businesses were required to comply with only one state data breach notification law—California's Database Breach Notification Security Act.[29] This law was the first of its kind and is the model for many other data breach notification laws in the United States.[30] California's statute remained the only data breach notification law until March 31, 2005, when a similar statute was passed in Arkansas.[31]

---

[27] A chronology of data breaches is available at *Chronology of Data Breaches*, PRIVACY RIGHTS CLEARINGHOUSE, http://www.privacyrights.org/data-breach (last updated Jan. 31, 2011).

[28] In 2008, three State Department employees opened President Obama's electronic passport file, violating the Department's privacy rules. *See* Helene Cooper, *State Dept. Finds Breaches of Obama's File*, N.Y. TIMES, Mar. 21, 2008, at A19.

[29] CAL. CIV. CODE § 1798.82 (West 2010).

[30] *See* Raymond G. Mullady, Jr. & Scott D. Hansen, *Identity Theft Litigation: A Roadmap for Defense and Protection*, 2008 UTAH L. REV. 563, 575.

[31] ARK. CODE ANN. §§ 4-110-101 to 108 (2010).

After the enactment of California's statute, businesses involved in interstate commerce had to decide whether to do just the bare minimum or whether to go beyond California's statutory requirements.[32] For instance, consider the situation in which a business that does not store customers' mailing addresses suffers a security breach. California's statute requires notification to California residents.[33] Determining whether a customer is a resident of California at the time of the breach would require this business to collect more information than it otherwise would have, thereby increasing the cost of doing business.[34] However, going beyond the requirements of the statute by notifying all of the affected customers could have unintended consequences on consumer opinion. Giving too many details about a possible breach to too many people could lead to a loss of consumer loyalty and a reduction in business.

California's use of vague and indefinite language—a by-product of legislators' ignorance regarding computers, the Internet, and technology—did not help businesses in making this decision.[35] Phrases in California's statute such as "reasonably believed"[36] and "in the most expedient time possible"[37] are vague and subject to interpretation.[38] The California legislature's failure to define these terms, as well as technical terms such as "encrypted," has left businesses uncertain as to whether the strength of their security policies is in proportion to the sensitivities of the types of data they collect.[39]

Businesses operating today must deal with the same questions as their counterparts in 2003; however, because many states have adjusted their statutes to rectify what they see as weaknesses in California's statutory language, the legal environment has become much more complicated. State

---

[32] *See* Timothy H. Skinner, *California's Database Breach Notification Security Act: The First State Breach Notification Law Is Not Yet a Suitable Template for National Identity Theft Legislation*, 10 RICH. J.L. & TECH. 1, 7 (2003).

[33] CAL. CIV. CODE § 1798.82(a).

[34] *See* Skinner, *supra* note 32, at 7–8.

[35] *See id.* at 8.

[36] CAL. CIV. CODE § 1798.82(a).

[37] *Id.*

[38] *See* Brandon Faulkner, Note, *Hacking into Data Breach Notification Laws*, 59 FLA. L. REV. 1097, 1110–11 (2007).

[39] *See* Skinner, *supra* note 32, at 11–12.

legislatures' attempts to rectify California's vague language have created a myriad of laws with differing requirements.

Any of the bills proposed in the 111th Congress would reduce the complicated statutory structure currently in place by preempting all of these state laws.[40] S. 139 and S. 1490 ("Senate bills") and H.R. 2221 were all introduced in previous sessions of Congress.[41] The two Senate bills have identical sections on notification.[42] H.R. 2221 and S. 3742 ("House-Senate bills") also have identical language on notification, with a few minor differences.[43] S. 3579 has the least comprehensive notification provision of them all, leaving much to federal agencies to regulate.[44]

These bills did not just suddenly appear. Senator Diane Feinstein of California introduced S. 139 back in 2003, soon after California's law was enacted.[45] She continues to support the bill, emphasizing that the threat of identity theft is growing and can no longer be ignored.[46] Senator Patrick Leahy of Vermont first introduced S. 1490 in 2005 with "high hopes of bringing urgently needed data privacy reforms to the American people."[47] H.R. 2221 was first introduced in the 109th Congress[48] and has since passed in the House.[49] If bills such as these have been on

---

[40] These bills require more than just notification in the event of a security breach. For instance, S. 1490 requires the implementation of data security programs and increased penalties for identity theft. *See* S. 1490, 111th Cong. (2009). However, analysis of these provisions is beyond the scope of this Note, which only examines the requirement of notification in the event of a data breach.

[41] *See* Personal Data Privacy and Security Act of 2007, S. 495, 110th Cong.; Notification of Risk to Personal Data Act of 2007, S. 239, 110th Cong.; Data Accountability and Trust Act, H.R. 958, 110th Cong. (2007).

[42] *See* S. 1490, 111th Cong. § 311 (2009); S. 139, 111th Cong. § 2 (2009).

[43] *See* S. 3742, 111th Cong. § 3 (2010); H.R. 2221, 111th Cong. § 3 (2009).

[44] *See* S. 3579, 111th Cong. § 4 (2010).

[45] 155 CONG. REC. S7871 (daily ed. July 22, 2009) (statement of Sen. Diane Feinstein).

[46] *Id.* ("According to a report by the Identity Theft Resource Center, the news media reported more than 620 breaches involving personal information during 2008. That works out to about one data security breach every 14 hours—and those are just the ones that are big enough to be covered in the media.").

[47] 155 CONG. REC. S7871 (daily ed. July 22, 2009) (statement of Sen. Patrick Leahy).

[48] *The Data Accountability and Trust Act: Hearing on H.R. 2221 and H.R. 1319 Before the H. Comm. on Energy and Commerce*, 111th Cong. 2 (2009) (statement of Rep. Bobby L. Rush).

[49] H.R. 2221, 111th Cong. (2009), *available at* http://www.govtrack.us/congress/bill.xpd?bill=h111-2221.

Congress's agenda since 2003, why is it taking so long for Congress to pass a data breach notification law?

As will be discussed in further detail below, data breach notification laws failed to pass in previous sessions of Congress because critics believe that many of the same deficiencies that plague California's law are also present in the federal bills. In order to understand these criticisms, it is necessary to first analyze the main elements of a data breach notification law.

B. The Elements of a Data Breach Notification Law

Every data breach notification law attempts to address the following major subjects: (1) the definition of "security breach" and the element of harm; (2) the definition of "personal information"; (3) who must be notified and when delivery must be completed; (4) how individuals must be notified and what information must be included in the notification; and (5) the penalties for failing to notify affected individuals. As will be discussed below, slight differences in language have a great impact on what businesses are required to do in the event of a security breach.

1. The Definition of a "Security Breach" and the Element of Harm

Whether to include the element of harm in the definition of "security breach" is the central issue in the debate over any data breach notification law. Many states have struggled with the fact that California's statute requires no additional element of harm to trigger notification.[50] Instead, the California statute defines "security breach" as the "unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the . . . business."[51] The trigger for notification is based on acquisition alone. Unauthorized acquisition or a "reasonable belief" that unauthorized acquisition has occurred is enough for the statute's notice requirements to apply.[52] Critics say that this

[50] *See* Brendan St. Amant, Recent Development, *The Misplaced Role of Identity Theft in Triggering Public Notice of Database Breaches*, 44 HARV. J. ON LEGIS. 505, 520–25 (2007).

[51] CAL. CIV. CODE § 1798.82(d) (West 2010).

[52] *Id.* § 1798.82(a).

could trigger over-notification, desensitizing the public to the severity of security breaches.[53]

New York has taken a different approach. While it does not require an additional element of harm, it does list several factors that can be used by businesses to determine "whether information has been acquired, or is reasonably believed to have been acquired, by an unauthorized person."[54] The factors are:

> (1) indications that the information is in the physical possession and control of an unauthorized person, such as a lost or stolen computer or other device containing information; or (2) indications that the information has been downloaded or copied; or (3) indications that the information was used by an unauthorized person, such as fraudulent accounts opened or instances of identity theft reported.[55]

Thus, New York has taken a middle-of-the road approach; it has elaborated upon California's law but has stopped short of requiring harm.

In contrast, states such as Louisiana, Missouri, and North Carolina have elected to add an additional element of harm, deciding that a risk of harm rather than an unauthorized acquisition should be the trigger for notification. In these states, notification is not required when businesses determine that identity theft is not likely to result,[56] "where illegal use of the personal information has [not] occurred or is [not] reasonably likely to occur or [where the breach] creates [no] material risk of harm to a consumer."[57]

Currently, businesses conducting interstate commerce that want to comply with all of the state notification laws can send letters to every individual whose personal information has been acquired or is reasonably believed to have been acquired by an unauthorized person, regardless of whether or not there is a significant risk of harm. In doing so, they choose the broadest trigger—California's trigger of unauthorized acquisition.[58] If they choose the broadest trigger, businesses do not need to ascertain whether each state's statutory language includes an element of harm, saving them both time and money. Thus,

---

[53] *See* Skinner, *supra* note 32, at 8–9.

[54] N.Y. GEN. BUS. LAW § 899-aa(1)(c) (McKinney 2010).

[55] *Id.*

[56] LA. REV. STAT. ANN. § 51:3074(G) (2010).

[57] *Cf.* N.C. GEN. STAT. § 75-61(14) (2010).

[58] CAL. CIV. CODE § 1798.82(a) (West 2010).

despite each state's attempt to limit unnecessary notification of consumers, among businesses conducting interstate commerce, there is really only one trigger—California's trigger.

The federal bills hoped to change this state of affairs. Although they do not significantly change California's definition of "security breach," they do include an additional element of harm. The Senate bills' definition is very similar to California's definition, defining "security breach" as a "compromise of the security, confidentiality, or integrity of computerized data through misrepresentation or actions that result in, or there is a reasonable basis to conclude has resulted in, acquisition of or access to [personal information] that is unauthorized or in excess of authorization."[59] Notification, however, is not required if a business: (1) conducts a "risk assessment" that "concludes . . . there is no significant risk that a security breach has resulted in, or will result in, harm to the individuals whose sensitive personally identifiable information was subject to the security breach"; (2) sends the results of the assessment to the Secret Service; and (3) receives no indication from the Secret Service that notification should still be given.[60] There is a presumption that there is no "significant risk" where information was encrypted or redacted.[61]

The House-Senate bills' definition is even simpler than the Senate bills', defining "security breach" rather simply as "unauthorized access to or acquisition of data in electronic form containing personal information."[62] No notification is required where the entity determines "that there is no reasonable risk of identity theft, fraud, or other unlawful conduct."[63] Once again, there is a presumption of no "reasonable risk" if the breached data is protected by encryption.[64]

S. 3579 adds significantly to this discussion, defining "breach of data security" as "the unauthorized acquisition of sensitive account information or sensitive personal information," while also including an exception for encrypted information.[65]

---

[59] S. 1490, 111th Cong. § 3(11)(A) (2009); S. 139, 111th Cong. § 13(6)(A) (2009).

[60] S. 1490 § 312(b)(1); S. 139 § 3(b)(1).

[61] S. 1490 § 312(b)(1); S. 139 § 3(b)(2). For a definition of "encryption," see *infra* note 88 and accompanying text.

[62] S. 3742, 111th Cong. § 5(1) (2010); H.R. 2221, 111th Cong. § 5(1) (2009).

[63] S. 3742 § 3(f)(1); H.R. 2221 § 3(f)(1).

[64] S. 3742 § 3(f)(2)(A); H.R. 2221, § 3(f)(2)(A).

[65] S. 3579, 111th Cong. § 2(3) (2010).

Notification is required only if, after an investigation, the entity determines that the breach is "reasonably likely to be misused in a manner causing substantial harm or inconvenience."[66] The bill even goes so far as to define the term "substantial harm or inconvenience" as "material financial loss to, or civil or criminal penalties imposed on, a consumer . . . ; or . . . the need for a consumer to expend significant time and effort to correct erroneous information relating to the consumer . . . , in order to avoid material financial loss, increase costs, or civil or criminal penalties."[67] The term does not include having to change an account number, and the harm must result from "identity theft or account fraud."[68]

2. The Definition of "Personal Information"

Like the term "security breach," the term "personal information" is highly debated. In California, "personal information" is defined as "an individual's first name or first initial and last name in combination with any" of the following: (1) a social security number; (2) a driver's license number or California identification card number; (3) an "[a]ccount number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to [the] individual's financial account"; and (4) medical or health insurance information.[69] In addition, either the individual's name or the information accompanying the individual's name must be "unencrypted."[70] The statute does not define the term "encrypted."[71]

This definition raises two issues. The first issue is whether the statute should cover only computerized data.[72] The Senate bills and the House-Senate bills apply only to computerized or electronic data.[73] S. 3579 makes no such distinction.[74] Some states have expanded their statutes to cover more than just

---

[66] *Id.* § 3(b)–(c).
[67] *Id.* § 2(11)(A).
[68] *Id.* § 2(11)(B).
[69] CAL. CIV. CODE § 1798.82(e) (West 2010).
[70] *Id.*
[71] *See* § 1798.82.
[72] *See* Skinner, *supra* note 32, at 10.
[73] S. 3742, 111th Cong. § 3(a) (2010); S. 1490, 111th Cong. § 3(11)(A) (2009); H.R. 2221, 111th Cong. § 3(a) (2009); S. 139, 111th Cong. § 13(6)(A) (2009).
[74] S. 3579, 111th Cong. § 3(c) (2010).

computerized data. For example, Indiana's statute "includes the unauthorized acquisition of computerized data that have been transferred to another medium, including paper, microfilm, or a similar medium, even if the transferred data are no longer in a computerized format."[75] Similarly, Massachusetts, which has passed one of the most progressive state privacy laws in the United States,[76] expanded its statute even further, covering "[a]ny material upon which written, drawn, spoken, visual, or electromagnetic information or images are recorded or preserved, regardless of physical form or characteristics."[77]

The second issue is whether California's definition of "personal information" is broad enough to protect consumers from identity theft.[78] New York has adopted a broader definition than California's, defining "personal information" as "any information concerning a natural person which, because of name, number, personal mark, or other identifier, can be used to identify such natural person."[79] However, the end result is not much different. New York distinguishes between "personal information" and "private information," the latter being defined in the same way California defines "personal information."[80] Because the statute applies only to businesses in possession of "private information,"[81] New York has not really altered California's original definition. Other states have been more progressive, opting to make specific additions to their statutes, including information such as taxpayer identification numbers, biometric data, and mothers' maiden names, in their lists of protected data.[82]

---

[75] IND. CODE § 24-4.9-2-2 (2010). Indiana also carves out a special exception for electronic data on portable devices, such as laptops, providing that a security breach "does not include . . . [u]nauthorized acquisition of a portable electronic device on which personal information is stored, if all personal information on the device is protected by encryption and the encryption key." *Id.*

[76] MASS. GEN. LAWS ch. 93H, § 1 (2010); *see also* Danzig et al., *supra* note 1, at 64.

[77] MASS. GEN. LAWS ch. 93H, § 1.

[78] *See* Amant, *supra* note 50, at 525–26.

[79] N.Y. GEN. BUS. LAW § 899-aa(1)(a) (McKinney 2010).

[80] *See* CAL. CIV. CODE § 1798.82(e) (West 2010); N.Y. GEN. BUS. LAW § 899-aa(1)(b).

[81] N.Y. GEN. BUS. LAW § 899-aa(2)–(3).

[82] *See, e.g.*, MD. CODE ANN., COM. LAW § 14-3501(d)(1)(iv) (LexisNexis 2010); NEB. REV. STAT. § 87-802(5)(e) (2010); N.D. CENT. CODE § 51-30-01(2)(a)(6) (2010).

Supporters of the federal bills agree that California's definition is too narrow. The House-Senate bills define "personal information" as "an individual's first name or initial and last name, or address, or phone number, in combination with any [one] or more of the following": (1) a social security number; (2) a driver's license or other state identification number; or (3) a "[f]inancial account number or credit or debit card number, and any required [code or password]."[83] Although this definition is very similar to California's definition, the bill leaves room for some flexibility, stating that the definition of "personal information" may be modified by the Federal Trade Commission ("FTC") "to accommodate changes in technology or practices."[84] The Senate bills go a bit further, deciding instead to make specific additions to the definition. Among the additions are a "passport number, or alien registration number, . . . [and] biometric data."[85] Any two of the following would also suffice in combination with the individual's name: (1) a "[h]ome address or telephone number"; (2) "[m]other's maiden name"; or (3) "[m]onth, day, and year of birth."[86] S. 3579 adds taxpayer identification numbers to its list of protected data.[87]

The federal bills also set forth another improvement—all of them, with the exception of S. 3579, offer a definition of encryption. The Senate bills and the House-Senate bills define encryption as "the protection of data in electronic form in storage or in transit using an encryption technology that has been adopted by an established standards setting body which renders such data indecipherable in the absence of associated cryptographic keys."[88] This definition provides consumers with more protection by precluding businesses from arguing that a simple eight-character password qualifies as encryption.

3. Who Must Be Notified and When Delivery Must Be Completed

With respect to both the "who" and the "when," data breach notification laws distinguish between businesses that own or

---

[83] S. 3742, 111th Cong. § 5(9)(A) (2010); H.R. 2221, 111th Cong. § 5(7)(A) (2009).
[84] S. 3742 § 5(9)(B); H.R. 2221 § 5(7)(B).
[85] S. 139, 111th Cong. § 13(7) (2009); S. 1490, 111th Cong. § 3(12) (2009).
[86] S. 139 § 13(7); S. 1490 § 3(12).
[87] S. 3579, 111th Cong. § 2(10)(A) (2010).
[88] S. 3742 § 5(5); S. 1490 § 3(7); H.R. 2221 § 5(4); S. 139 § 13(4).

license personal information ("Owners") and businesses that maintain personal information that is owned and licensed by others ("Maintainers"). This distinction is made, presumably, to prevent any confusion over which entity is responsible for giving notice in the event that both entities are victims of the same breach. For instance, California's law provides that following the occurrence of a security breach, Owners must notify "any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person,"[89] while Maintainers need only inform "the owner or licensee of the information" in question.[90]

The Senate bills and the House-Senate bills also distinguish between Owners and Maintainers. Like California, the House-Senate bills require a Maintainer to notify only the Owner.[91] Owners, on the other hand, must "notify each individual who is a citizen or resident of the United States whose personal information was acquired or accessed as a result of such a breach of security."[92] The Senate bills are very different. Unless an agreement is made between the Owner and the Maintainer, the Maintainer must notify both the Owner and any affected residents, or risk violating the act.[93] The Maintainer is only relieved of this duty when the Owner notifies the affected individuals first.[94] Presumably, should one of the Senate bills pass, most Owners and Maintainers would amend their contracts to make it clear which entity is responsible for sending notice because clarifying this separation of duties would avoid confusion and help protect the parties from liability. The language of S. 3579 does not distinguish between Owners and Maintainers. Instead, both Owners and Maintainers are considered "covered entit[ies]" and must notify "all consumers to whom the [personal information] relates."[95]

In addition to notifying affected consumers, many states also require entities to notify a consumer reporting agency when a certain threshold number of individuals has been affected to allow for the maintenance of information on such breaches at a

---

[89] CAL. CIV. CODE § 1798.82(a) (West 2010).
[90] *Id.* § 1798.82(b).
[91] S. 3742 § 3(b)(1); H.R. 2221 § 3(b)(1).
[92] S. 3742 § 3(a)(1); H.R. 2221 § 3(a)(1).
[93] S. 1490 § 311(a)–(b); S. 139 § 2(a)–(b).
[94] S. 1490 § 311(b)(3); S. 139 § 2(b)(3).
[95] *See* S. 3579, 111th Cong. §§ 2(7)(A), 3(c)(1) (2010).

national level.[96] The Senate bills and S. 3579 include similar provisions. If over 5,000 individuals have been affected by a breach, notice must also be given to consumer reporting agencies.[97] The House-Senate bills have no comparable provision.

In certain circumstances, some states also require that parties inform the state attorney general.[98] At the state level, private sector lobbyists have succeeded in states such as Indiana, where they were able to block an amendment that would have required notification to the state attorney general, who could then post information regarding the breach on a website.[99] "Lobbyists decried the provision, claiming it would provide phishers a golden opportunity to prey on unsuspecting consumers. The phishers would use the site against its intended purpose, lobbyists argued, by targeting visitors and getting them to input personal information."[100] Microsoft, AT&T, and Verizon were among those objecting to the Indiana bill.[101] Governor Arnold Schwarzenegger of California blocked a similar amendment in October 2010.[102]

In addition to consumers and consumer reporting agencies, other entities must be notified as well. The House-Senate bills require that Owners notify the FTC;[103] the Senate bills require business to notify the United States Secret Service and the

---

[96] *See, e.g.*, FLA. STAT. § 817.5681(12) (2005). A consumer reporting agency is an "agency that compiles and maintains files on consumers on a nationwide basis." 15 U.S.C. § 1681a(p) (2006). It must "regularly engage[ ] in the practice of assembling . . . and maintaining, for the purpose of furnishing consumer reports to third parties bearing on a consumer's credit worthiness, credit standing, or credit capacity, each of the following . . . : (1) [p]ublic record information [and] (2) [c]redit account information." *Id.*

[97] S. 3579 § 3(c)(1)(D); S. 1490 § 315; S. 139 § 6.

[98] *See, e.g.*, N.C. GEN. STAT. § 75-65(f) (2009) (requiring notification to the Attorney General where 1,000 or more consumers are involved).

[99] Bruce E. H. Johnson & Sarah K. Duran, *Recent Developments in Commercial Speech and Consumer Privacy Interests*, *in* PATENTS, COPYRIGHTS, TRADEMARKS, AND LITERARY PROPERTY COURSE HANDBOOK SERIES 53, 69 (2008).

[100] *Id.*

[101] Chris Soghoian, *Industry Giants Lobby To Kill Pro-Consumer Data-Breach Legislation*, CNET NEWS (Feb. 5, 2008), http://news.cnet.com/8301-13739_3-9865076-46.html.

[102] Letter from Arnold Schwarzenegger, Gov. of Cal., to the Members of the Cal. State Senate (Oct. 10, 2009) (vetoing S. 20), *available at* http://info.sen.ca.gov/pub/09-10/bill/sen/sb_0001-0050/sb_20_vt_20091011.html.

[103] S. 3742, 111th Cong. § 3(a)(2) (2010); H.R. 2221, 111th Cong. § 3(a)(2) (2009).

media,[104] and S. 3579 requires "covered entities" to notify: (1) a designated federal agency; (2) a law enforcement agency; and (3) any entity that owns "a financial account to which the [personal information] relates."[105]

States have gone different ways with regard to when notification must be sent. In California, whereas Owners must notify residents "in the most expedient time possible and without unreasonable delay,"[106] Maintainers must notify the Owners "immediately."[107] Delays to accommodate the "needs of law enforcement [in conducting a criminal investigation] . . . or . . . to determine the scope of the breach and restore the reasonable integrity of the data system" are considered reasonable.[108] A few states have declined to follow California's approach, deciding instead on a bright line rule. For example, Florida and Ohio both require notification within forty-five days.[109]

With respect to timing, the Senate bills and the Senate-House bills have taken different paths. The Senate bills retain California's vague language, requiring businesses to deliver notification "without unreasonable delay following the discovery . . . of a security breach."[110] As in California, delays to accommodate the need to "determine the scope of the security breach, prevent further disclosures, and restore the reasonable integrity of the data system" or to accommodate the needs of law enforcement are considered reasonable.[111] The House-Senate bills, on the other hand, make an attempt at clarification, requiring businesses to provide notice within sixty days absent "extraordinary circumstances," while still accommodating the needs of law enforcement and national security agencies.[112]

---

[104] S. 1490, 111th Cong. §§ 313(2), 316 (2009); S. 139, 111th Cong. §§ 4(2), 7 (2009).

[105] S. 3579, 111th Cong. § 3(c)(1)(C) (2010).

[106] CAL. CIV. CODE § 1798.82(a) (West 2010).

[107] *Id.* § 1798.82(b).

[108] *Id.* § 1798.82(a).

[109] FLA. STAT. § 817.5681(1)(a) (2010); OHIO REV. CODE ANN. § 1347.12(B)(2) (LexisNexis 2010) (covering government agencies); *id.* § 1349.19(B)(2) (covering private entities).

[110] S. 1490, 111th Cong. § 311(c)(1) (2009); S. 139, 111th Cong. § 2(c)(1) (2009).

[111] S. 1490 § 311(c)(2), (d); S. 139 § 2(c)(2), (d).

[112] S. 3742, 111th Cong. § 3(c) (2010); H.R. 2221, 111th Cong. § 3(c) (2009).

S.3579 has failed to address this topic, giving federal agencies the power to issue regulations regarding the standards that should apply.[113]

4. How Individuals Must Be Notified and What Information Must Be Included in the Notification

Any data breach notification law must address the manner in which notification may be given. California's statute provides that notification may be given via "written notice" or via "electronic notice."[114] The same is said in the House-Senate bills.[115] S. 3579 and the Senate bills similarly allow notice to be given in writing or via e-mail and additionaly permit notice by telephone.[116]

In California, "substitute notice" is permitted if the entity "demonstrates that the cost of providing notice would exceed [$250,000], or that the affected class of subject persons to be notified exceeds 500,000, or the [entity] does not have sufficient contact information" to provide direct notice.[117] "Substitute notice" consists of an e-mail, a "conspicuous" posting on the entity's website, and notification to statewide media.[118] The House-Senate bills also allow for "substitute notice" but only in narrow circumstances—when the database in question contains the information of fewer than 1,000 people and direct notification cannot be given due to excessive cost or a "lack of sufficient contact information for the individual required to be notified."[119] According to the House-Senate bills, the notification need only inform consumers that they may receive two years of free credit reports in certain circumstances and a telephone number by which they can learn if their personal information has been compromised.[120] S. 3579 also allows for "substitute notice," but it is less clear than the House-Senate bills, leaving the details to federal agencies to regulate.[121] The Senate bills contain no provision allowing for "substitute notice."

---

[113] *See* S. 3579, 111th Cong. § 4(e) (2010).
[114] CAL. CIV. CODE § 1798.82 (g)(1)–(2) (West 2010).
[115] S. 3742 § 3(d)(1)(A); H.R. 2221 § 3(d)(1)(A).
[116] S. 3579 § 4(c)(2)(A); S. 1490 § 313(1)(B); S. 139 § 4(1)(B).
[117] CAL. CIV. CODE § 1798.82 (g)(3).
[118] *Id.*
[119] S. 3742 § 3(d)(2)(A)(ii); H.R. 2221 § 3(d)(2)(A)(ii).
[120] S. 3742 § 3(d)(2)(C); H.R. 2221 § 3(d)(2)(C).
[121] *See* S. 3579 § 4(c)(2)(B).

State statutes vary with regard to what information must be included in the notice. On this subject, California is silent.[122] Therefore, the letters and e-mails sent to California residents do not need to be very specific. Specific disclosure is only required upon the affected resident's request.[123] Other states have filled in this gap, requiring businesses to provide affected individuals with descriptions of the breach, the types of personal information compromised, contact information for consumer reporting agencies, and various tips on how to prevent identity theft.[124]

On this subject, the House and Senate seem to agree that California's law is too vague. The House-Senate bills provide that notification must include: (1) a description of the personal information compromised; (2) a telephone number for the business; (3) notice that the individual may receive two years of free credit reports in certain circumstances; (4) the addresses and toll-free numbers for credit reporting agencies; and (5) the website and the toll-free number for the FTC.[125] Similarly the Senate bills require that each notice include:

> (1) a description of the categories of sensitive personally identifiable information that was, or is reasonably believed to have been . . . acquired by an unauthorized person; (2) a toll-free number [through which the individual can contact the business for more information]; and (3) the toll-free contact telephone numbers and addresses for the major credit reporting agencies.[126]

In addition, individual states may require the inclusion of information regarding "victim protection assistance" provided in their particular states.[127] Once again, the drafters of S. 3579 declined to take the initiative in this area, leaving much of the planning to federal agencies; nevertheless, they do require that there be: (1) a description of the personal information that was

---

[122] *See* CAL. CIV. CODE § 1798.82.

[123] *Id.* § 1798.83(a).

[124] *See, e.g.*, IOWA CODE ANN. § 715C.2(5) (West 2010); MD. CODE ANN., COM. LAW § 14-3504(g) (West 2010).

[125] S. 3742 § 3(d)(1)(B); H.R. 2221 § 3(d)(1)(B). Here, the language in the two bills diverges slightly with S. 3742 also requiring that the notice contain "the date, estimated date, or estimated date range of the [security breach]." S. 3742 § 3(d)(1)(B)(i).

[126] S. 1490, 111th Cong. § 314(a) (2009); S. 139, 111th Cong. § 5(a) (2010).

[127] S. 1490 § 314(b); S. 139 § 5(b).

breached; (2) a description of what the business has done to secure that information; and (3) a summary of the victim's rights.[128]

5. The Penalties for Failing To Notify Affected Individuals

Another subject of contention is whether individuals should be allowed a private right of action against businesses that fail to notify them of a security breach.[129] Allowing a private right of action can create an increased incentive for businesses to comply with state law; however, the benefits to plaintiffs are limited. These lawsuits are usually based on claims of negligence or breach of contract.[130] Therefore, plaintiffs are required to show more likely than not that the breach—the failure to notify—caused the plaintiff's injuries.[131] This places an extremely heavy burden on the plaintiff. California permits any customer injured by a violation of the notification law to sue the offending business and recover damages.[132] In addition to California, ten states and the District of Columbia allow a private right of action,[133] but in many states, only the state attorney general may sue for a failure to comply.[134]

None of the federal bills allow for a private right of action. The Senate bills, however, do allow the United States Attorney General to bring a civil action against businesses that violate the act for damages not to exceed $1,000 per day, per individual up to a maximum of $1,000,000 per violation.[135] In addition, the Attorney General may apply to the court to enjoin businesses from violating the statute's requirements.[136] The Senate bills also allow state attorneys general to bring actions against businesses when they believe that "an interest of the residents of [their] State[s] has been or is threatened or adversely affected by the engagement of a business entity in a practice that" violates

---

[128] S. 3579, 111th Cong. § 4(d) (2010).

[129] *See* Skinner, *supra* note 32, at 14.

[130] *Id.*

[131] *Id.*

[132] CAL. CIV. CODE § 1798.84(b) (West 2010).

[133] SCOTT P. COOPER ET AL., *State Privacy Laws*, *in* PROSKAUER ON PRIVACY 2010, § 5:5.5[B][9] (PLI 2010) (District of Columbia, Louisiana, Maryland, New Hampshire, New Jersey, North Carolina, South Carolina, Tennessee, Texas, Virginia, and Washington).

[134] *See, e.g.*, N.Y. GEN. BUS. LAW § 899-aa(6)(a) (McKinney 2010).

[135] S. 1490, 111th Cong. § 317(a) (2009); S. 139, 111th Cong. § 8(a) (2010).

[136] S. 1490 § 317(b); S. 139 § 8(b).

the act.[137] However, no state attorney general may bring such an action at the same time as the United States Attorney General.[138] The penalties for violating House-Senate bills are similar to the penalties in the Senate bills. However, the FTC, rather than the Attorney General, would commence the civil action,[139] and the maximum civil penalty cannot exceed $5,000,000.[140] Furthermore, according to the House-Senate bills any violation would be treated as an "unfair and deceptive act" under 15 U.S.C. 57a(a)(1)(B).[141] S. 3579 relies on administrative enforcement and precludes state attorneys general from instituting civil or criminal actions.[142]

II. ANALYZING LOBBYISTS' PERSPECTIVES ON PREEMPTION

With regard to lobbyists and special interests, the main debate is whether a federal data breach notification law should preempt the many state laws currently in place.[143] Once again, this Note argues that a strict federal data breach notification law that preempts state laws will provide increased protection to consumers in the United States.

While industry groups and consumer protection groups support the creation of a federal law,[144] the latter do not want states to lose the power to enact stricter protections than the

---

[137] S. 1490 § 318; S. 139 § 9.

[138] S. 1490 § 318(c); S. 139 § 9(c).

[139] S. 3742, 111th Cong. § 4(b) (2010); H.R. 2221, 111th Cong. § 4(b) (2009).

[140] S. 3742 § 4(c)(2)(C)(ii); H.R. 2221 § 4(c)(2)(C)(ii).

[141] S. 3742 § 4(b)(1); H.R. 2221 § 4(b)(1).

[142] S. 3579, 111th Cong. § 5 (2010).

[143] *See* Lee, *supra* note 13, at 143–44.

[144] *See* Letter on S. 1490, *supra* note 21 ("The U.S. has a national economy, and almost every state has enacted various data security and breach notification provisions, many of which differ from one another in material ways. A federal security breach notification standard that is not only inconsistent with these laws, but also with other federal laws would create regulatory uncertainty and require notification in circumstances where individuals face no risk of identity theft or financial harm."); Letter on H.R. 2221, *supra* note 21 ("We [the undersigned leading consumer groups] applaud the sponsors for including in the bill some of the strongest public policy provisions of any bill before the Congress to address the myriad data security and privacy problems that have been identified following years of well-publicized security breaches at some of the nation's largest firms."); Letter from Michael W. Macleod-Ball, Acting Director, ACLU, to Patrick Leahy, Chairman, Sen. Judiciary Comm. & Jeff Sessions, Ranking Member of Sen. Judiciary Comm. 6 (Nov. 2, 2009), *available at* http://www.aclu.org/files/assets/ltr_support_S1490.pdf ("We support S. 1490 because it is a common sense effort to regulate an industry that desperately needs it.").

federal government.[145] On the industry side, the Securities Industry Association, Nationwide Mutual Insurance Co., and Microsoft have all expressed their support for federal legislation.[146] These groups hope to increase certainty and reduce the confusion that comes with complying with so many state laws.[147] They hope to secure a weak federal law that preempts state laws.[148]

On the other side of the debate are consumer protections groups, which, in true Jeffersonian fashion, do not want a federal law to preempt the various state laws.[149] According to groups such as the Center for Digital Democracy, the U.S. Public Interest Research Group ("PIRG"), the Consumer Federation of America, the Electronic Frontier Foundation, and the Privacy Rights Clearinghouse, a "federal law should always serve as a floor, not a ceiling."[150] These groups argue that the states provide a valuable laboratory for the creation of public policy and should not be prohibited from experimenting.[151]

---

[145] Letter on H.R. 2221, *supra* note 21 ("[T]he bill . . . includes unacceptable preemptive language . . . , despite strong evidence that the states have led . . . on identity theft and other privacy protection issues.").

[146] Lee, *supra* note 13, at 143–44.

[147] *See id.*

[148] *See* Letter on S. 1490, *supra* note 21 ("We [the undersigned industry groups] believe that this legislation should exempt entities covered by other federal security breach and data security laws and that the preemption standards should explicitly preempt all state laws relating to any activity covered under this Act."). The private sector has spent a lot of money fighting on this issue. When the Lobbying Disclosure Act Database is searched, ChoicePoint, eBay Inc., Bank of America, N.A., and Microsoft are just a few of the entities that appear. Although these filings do not indicate which side of the debate these entities are on, it is clear that many large private sector entities are willing to spend on this issue. In 2006, the year after it suffered that devastating breach, ChoicePoint reported that it spent $588,000 lobbying on its own behalf regarding data breach legislation in both the House and the Senate. That same year, eBay Inc. reported spending more than $1,085,000 on lobbying. Some of this money was spent on bills introduced in the 109th Congress to address data security. Bank of America, N.A., which spent a total of $1,020,000 in the second half of 2006, reports spending money on some of the same bills. The Lobbying Disclosure Act Database can be found at http://soprweb.senate.gov/index.cfm?event=choosefields.

[149] Lee, *supra* note 13, at 143.

[150] Letter on H.R. 2221, *supra* note 21.

[151] *Id.*; *see also* Flora J. Garcia, Note, *Data Protection, Breach Notification, and the Interplay Between State and Federal Law: The Experiments Need More Time*, 17 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 693, 726 (2007) ("State laws are beginning to address the remedies at the roots of the malady, the laissez-faire attitudes of some companies and agencies about data security and protection, and a marketplace with many different approaches is a robust test of what the best

Unfortunately, this debate has hindered the development of a federal data breach notification law for too long. As already stated, the myriad of state laws currently in place has created a complex legal environment for businesses that are victims of security breaches. As victims, businesses should not be forced to bear all the costs.[152] If a federal law does not come to fruition, businesses will continue to be hounded with complicated questions resulting from a thorny statutory scheme. In an age where e-commerce and the Internet have become important means of conducting business, such complications severely increase the costs of operating in the United States and lead to uncertainty and hesitation.

The debate over a federal data breach notification law is not necessarily the best arena for ensuring that businesses take on the proper burden. Although the private sector is in the best position to prevent security breaches from happening,[153] it is difficult to determine whether notification laws have actually had a significant impact on reducing the occurrence of breaches.[154]

---

remedies will be at this still-nascent point in the development of electronic data storage."). This is a common argument in the arena of consumer protection law. For instance, professors of consumer law and banking law who support the creation of a federal Consumer Financial Protection Agency argue that the merits of preemption

> are outweighed by the value of having states operate as laboratories . . . . It is important that Congress not take a simplistic approach favoring only federal development of consumer protection laws . . . ; and that Congress not limit the role of the states to enforcement of state and federal law. State legislatures and courts need to be able to continue to develop consumer protection law . . . . In addition, problems are much more likely to grow larger if they can be addressed only at the federal level and not also by states where they first appear.

Richard M. Alderman et al., *A Communication from Academic Faculty Who Teach Courses Related to Consumer Law and Banking Law at American Law Schools* 5 (Sept. 29, 2009), http://law.hofstra.edu/pdf/Media/consumer-law%209-28-09.pdf.

[152] *See* Lilia Rode, Comment, *Database Security Breach Notification Statutes: Does Placing the Responsibility on the True Victim Increase Data Security?*, 43 HOUS. L. REV. 1597, 1627 (2007).

[153] Kathryn E. Picanso, Note, *Protecting Information Security Under a Uniform Data Breach Notification Law*, 75 FORDHAM L. REV. 355, 390 (2006).

[154] *See* S. Kasim Ravzi, Comment, *To What Extent Should State Legislatures Regulate Business Practices as a Means of Preventing Identity Theft?*, 15 ALB. L.J. SCI. & TECH. 639, 657–58 (2005). A study on breach notifications conducted by the Ponemon Institute revealed that thirty-nine percent of respondents believed the notification was "junk mail, spam or a telemarketing phone call" and that fifty percent of the respondents still did nothing new to protect themselves against identify theft. Ponemon Inst. LLC, *National Survey on Data Security Breach Notification* 10, 17 (2005), *available at* http://www.whitecase.com/files/

Advances in technology and the development of new business practices have also had an effect.[155] Therefore, lobbyists' energies may be better spent in areas that will increase the use of such technologies and practices.

In addition, fighting preemption has left the residents of some states completely unprotected. Even now, over four years after the ChoicePoint breach, businesses in four states—Alabama, Kentucky, New Mexico, and South Dakota—are not required to notify individuals when their personal information has been compromised. Even though two of these states, Alabama and Kentucky, reported that in 2007, Internet related complaints were among the top ten consumer complaints received by their attorneys general,[156] legislators in these states remain idle. Although "[s]tate legislatures . . . need to be able to continue to develop consumer protection law,"[157] in general, the experiment should be over with regard to notification. Congress should not have to wait until these states decide to protect their consumers when it has the ability to protect them now.

III. THE COMPROMISE: A STRICT DATA BREACH NOTIFICATION LAW THAT PREEMPTS STATE LAWS

The best way to protect consumers' personal information is to implement a strict federal data breach notification law that preempts the forty-six state laws currently in place. A strict federal law would increase incentives for businesses to comply by reducing the cost of compliance and increasing the reputational harm associated with security breaches. Increased notification gives consumers more control over their own personal information. The following discussion is broken up into two parts. Part A discusses the goal of this law—increased consumer control. Part B revisits the five major elements of a data breach notification law, making recommendations on the form each element should take at the federal level.

FileControl/863d572d-cde3-4e33-903c-37eaba537060/7483b893-e478-44a4-8fed-f49aa917d8cf/Presentation/File/Security_Breach_Survey%5B1%5D.pdf.

[155] Ravzi, *supra* note 154.

[156] REECE RUSHING, ARI SCHWARTZ & ALISSA COOPER, CTR. FOR AM. PROGRESS & CTR. FOR DEMOCRACY & TECH., ONLINE CONSUMERS AT RISK AND THE ROLE OF STATE ATTORNEYS GENERAL 9 (2008), *available at* http://cdt.org/privacy/20080812_ag_consumer_risk.pdf.

[157] Alderman et al., *supra* note 151, at 5.

A. The Goal: Increasing Consumers' Ability To Control Their Personal Information

A strict federal data breach notification law will increase consumers' ability to control their personal information. In the context of informational privacy,

> [c]ontrol . . . refers to the fact that it is in many respects in a person's hands—and in other respects she can at least guess—what others know about her in any particular instance, that she can thus make well-founded assumptions concerning what the people or institutions she deals with know about her, and that in accordance with these assumptions and expectations she may also possess corresponding possibilities for penalizing or at least criticizing infractions.[158]

Increasing consumer control involves two important policy goals. First, a consumer can only have control over his or her personal information if he or she knows who is in possession of it; therefore, increased control requires increased disclosure. Disclosure "helps the market to function properly by assisting customers when choosing whether to deal with (or stop dealing with) a particular institution."[159] Without a strict law, most businesses will disclose as little as possible.[160] They do not want to see their revenue decrease after "40% of consumers consider[ ] discontinuing their relationship with [them]."[161] Thus, any federal law must contain language ensuring that businesses do not have a way of escaping their notification requirements. In addition, it must be specific about what information businesses are required to disclose. The more detail included in the notification, the more control a person has over his or her personal information. An added benefit of increased disclosure is that it will aid in deterring hackers and identity thieves from violating the law.[162] If individuals are put on notice that their personal information has been accessed, they will be much more vigilant, reviewing their banking statements and ordering credit reports. Because notified individuals are more likely to report discrepancies, hackers are more likely to get caught.

---

[158] BEATE ROSSLER, THE VALUE OF PRIVACY 111 (2005) (internal quotation marks omitted).

[159] Janger & Schwartz, *supra* note 11, at 234.

[160] *See* Amant, *supra* note 50, at 523–24.

[161] *Id.* at 517.

[162] *Id.* at 524.

Second, increased control requires that the federal government give businesses more of an incentive to improve security by increasing reputational costs.[163] Statistical analyses show that "[t]he challenged macroeconomic backdrop" is causing companies to cut back in all areas, including security.[164] Companies continue to reduce information security budgets and many do not have privacy programs in place.[165] This is occurring even though many system attacks are not difficult to prevent.[166] Poor information security leads not only to an increased number of breaches but also to long delays in determining how the breach occurred. Although there is no statistically significant data proving that data breach laws reduce levels of fraud and identity theft,[167] strict statutes still have the ability to encourage businesses to take preventative measures to prevent the reputational harm that results from a breach. A lax federal notification law, on the other hand, will do nothing to increase investment in security. Instead, it will signal to businesses that the federal government is not concerned about consumer privacy.

B. Recommendations for a Federal Law

Keeping the goal of increasing consumer control in mind, this Part revisits the five major elements of a data breach notification law: (1) the definition of "security breach" and the element of harm; (2) the definition of "personal information"; (3) who must be notified and when delivery must be completed;

---

[163] See generally Paul M. Schwartz & Edward J. Janger, *Notification of Data Security Breaches*, 105 MICH. L. REV. 913, 929 (2007), for more on reputational costs.

[164] *See, e.g.*, DELOITTE, LOSING GROUND: 2009 TMT GLOBAL SECURITY SURVEY 3 (2009), *available at* http://www.deloitte.com/assets/Dcom-Norway/Local%20Assets/Documents/tmt_securitysurvey2009.pdf.

[165] *See id.* at 5 (noting that, among the surveyed companies, thirty-two percent reduced their information security budget, while twenty-five percent raised their budget less than five percent). These declining or minimally increasing security investments may not be enough to keep pace with the growing list of challenges, emerging technologies, and increasingly sophisticated attacks. Baker et al., *supra* note 26, at 39 (finding that only twenty-eight percent of victims had an incident response system in place).

[166] *See* Baker et al., *supra* note 26, at 3 ("Most of these incidents do not require difficult or expensive preventative controls; mistakes and oversight hinder security efforts more than a lack of resources.").

[167] *See* Alana Maurushat, *Data Breach Notification Law Across the World from California to Australia* (Univ. of New South Wales Faculty of Law Research Series, Paper 11, 2009), *available at* http://law.bepress.com/cgi/viewcontent.cgi?article=1153&context=unswwps.

(4) how individuals must be notified and what information must be included in the notification; and (5) the penalties for failing to notify affected individuals.[168]

1. The Definition of a "Security Breach" and the Element of Harm

With regard to what level of harm should trigger notification, California's approach with a slight modification is still the best way to increase disclosure while retaining the important incentive of reputational harm. California's statute provides that unauthorized acquisition or a "reasonable belief" that unauthorized acquisition has occurred is enough for the statute's notice requirements to apply.[169] Despite criticisms that a broad trigger will increase attacks by phishers—criminals who send fraudulent e-mails to gather the personal information of unsuspecting individuals—it is inevitable that illegitimate companies will try to gather consumers' personal information in an attempt "to exploit those who they perceive as being vulnerable to attack."[170] Opportunistic criminals will do this whether or not a federal data breach notification law is passed. Therefore, such criticisms should not be a reason for blocking the passage of a federal law.

To reduce the vagueness of California's language, any proposed federal statute should include factors for determining when there is a "reasonable belief" that unauthorized acquisition has occurred. Although this stops short of requiring an additional element of harm, it narrows the trigger language and helps clarify the law. The factors presented in New York's statute would be a good starting point. Once again, the factors are:

> (1) indications that the information is in the physical possession and control of an unauthorized person, such as a lost or stolen computer or other device containing information; or (2) indications that the information has been downloaded or

---

[168] *See* discussion *supra* Part I.B.

[169] *See* CAL. CIV. CODE § 1798.82(a) (West 2010).

[170] ANDREW SERWIN, INFORMATION SECURITY AND PRIVACY: A PRACTICAL GUIDE TO FEDERAL, STATE AND INTERNATIONAL LAW § 25:2 (2010).

> copied; or (3) indications that the information was used by an unauthorized person, such as fraudulent accounts opened or instances of identity theft reported.[171]

However, businesses should not be in control of weighing these factors.[172] Giving businesses this power without oversight would be tantamount to applying the business-judgment rule in a situation where businesses clearly have an interest in self-preservation.[173] An exemption allowing entities to conduct their own investigation to determine whether there is a "significant risk of harm,"[174] though favorable to industry lobbyists, would likely severely decrease the number of instances in which notification is required. Thus, consumer protection groups are justified in their "dislike [of] trigger language that narrows notification to occurrences where there is a reasonable belief of a significant risk of identity theft because . . . the standard would allow companies to notify only certain select individuals, leaving others at risk."[175] According to the Consumer Program Director of PIRG, "[t]he fact that the company doesn't yet know whether or how the information will be misused should not be enough to excuse notice."[176]

The last word on whether there is a reasonable belief of unauthorized acquisition should be with a new federal agency specializing in investigating security breaches rather than with the businesses themselves.[177] The FTC currently does not have enough authority to take on this role because its jurisdiction is limited—other federal agencies have jurisdiction over entities such as financial institutions.[178] This new agency must be equipped with the resources and technology to make determinations within a relatively short period of time and must

---

[171] N.Y. GEN. BUS. LAW § 899-aa(1)(c) (McKinney 2010).

[172] *See* Amant, *supra* note 50, at 506.

[173] The business-judgment rule is the "presumption that in making business decisions not involving direct self-interest or self-dealing, corporate directors act on an informed basis, in good faith, and in the honest belief that their actions are in the corporation's best interest." BLACK'S LAW DICTIONARY 226 (9th ed. 2009).

[174] A similar exemption is present in the Senate bills. *See* discussion *supra* Part I.B.1.

[175] Lee, *supra* note 13, at 145.

[176] Edmund Mierzwinski, *Testimony of Consumer and Privacy Groups on Data Security, Data Breach Notices, Privacy and Identity Theft*, at 330, 340 (PLI Corp. Law & Practice Course Handbook Series, No. 8565, 2006).

[177] *See* SERWIN, *supra* note 170.

[178] *See id.*

be given the power to enforce its decisions. Otherwise, consumers will bear the costs of not being notified until it is too late. Adding this extra level of review will increase consumer protection by ensuring that businesses suffering from a breach comply with the law. Businesses will not be allowed to make their own exceptions.

Critics arguing that the absence of a harm requirement will lead to over-notification and unnecessary increases in the cost of doing business presume that the benefits of over-notification do not exceed the costs.[179] In fact, the opposite is true. First, requiring an element of harm has not been able to prevent the public from becoming desensitized to notification letters. Junk mail already inundates American mailboxes, and half of the public ignores notification letters.[180] It is unlikely that a federal law will change these problems. Thus, all things being equal, a federal law with a broad trigger will increase the number of consumers that are aware that their information has been compromised. Second, although some analysts argue that a broad trigger will discourage disclosure by increasing reputational risk,[181] this problem is rectified by requiring a federal agency to review whether there is a "reasonable belief" of unauthorized acquisition. This agency would be able to overcome businesses' reluctance to comply by enforcing the federal law and perhaps even by conducting audits of businesses' data breach procedures. Ultimately, a broad trigger will ensure that those who should receive notification do receive notification, thereby increasing disclosure, promoting knowledge, and improving consumers' control over their personal information.

2. The Definition of "Personal Information"

As discussed above, there are two main issues that arise with regard to the definition of "personal information"—(1) whether the statute should protect only computerized data; and (2) whether the definition of "personal information" is sufficiently broad to protect consumers from identity theft.[182] With regard to the first issue, PIRG maintains that it will not

---

[179] *See* Amant, *supra* note 50, at 524.

[180] *See* Rode, *supra* note 152, at 1626.

[181] *See, e.g.*, Janger & Schwartz, *supra* note 11 (suggesting that fear of liability may encourage nondisclosure).

[182] *See* discussion *supra* Part I.B.2.

support any federal law unless it covers both electronic and paper data.[183] PIRG's request is reasonable. Because "personal information" remains sensitive whether it is on paper or saved on a computer hard drive, it makes no sense to protect one form of information and not the other. Businesses are in the best position to make sure that all the personal information they collect is stored safely and disposed of properly. Therefore, Massachusetts's statute, which covers "[a]ny material upon which written, drawn, spoken, visual, or electromagnetic information or images are recorded or preserved, regardless of physical form or characteristics,"[184] is a good model for the federal law to follow.

With regard to the second issue, a strict federal law must contain a flexible definition of "personal information" to be effective. Many types of information can lead to identity theft. Thus, the law must be able to adapt when criminals change targets.[185] For example, an e-mail address in combination with a mother's maiden name, could reasonably allow a hacker to access an individual's personal account on various websites, including those used for banking and insurance.[186] Because a reasonable business should conclude that the unauthorized acquisition of an individual's e-mail address in combination with a mother's maiden name could lead to identity theft, this information should be protected by federal law. In this instance, a simple notification letter would give consumers control over their personal data by prompting them to change their account passwords and their security questions. None of the federal bills in the 111th Congress addressed this issue.

One way to keep the definition flexible is to adopt a modified version of New York's general definition of "personal information." "Personal information" should be defined as "any information concerning a natural person which, because of name,

---

[183] *See* Lee, *supra* note 13, at 144.

[184] MASS. GEN. LAWS ANN. ch. 93, § 1(a) (West 2010).

[185] *See* Baker et al., *supra* note 26 ("As supply has increased and prices have fallen, criminals have had to overhaul their processes and differentiate their products in order to maintain profitability.").

[186] Many websites have a "forgot password?" link, allowing the user to enter an e-mail address and "security question," such as "what is your mother's maiden name," when they have forgotten their personal password. The organization then sends the user a new password through their e-mail address. Anyone who knows the user's e-mail address and the answer to the user's security question can then gain access to the user's account.

number, personal mark, or other identifier, can *reasonably* be used to identify such natural person."[187] The law should also enumerate types of data that are per se "personal information." Social security numbers, state identification card numbers, driver's license numbers, and account numbers along with any necessary codes or passwords needed to access the accounts, should all be included on this list. In addition, the new federal agency discussed above should be given leave to add other sensitive categories of information to this list by issuing separate regulations.[188] In this way, federal agencies, the courts, and the legislature will be given the flexibility to adjust the definition of "personal information" as necessary to accommodate changes in technology and new trends in identity theft.

3. Who Must Be Notified and When Delivery Must Be Completed

In Part I.B.3, this Note explored how data breach notification statutes, following California's statute, have split responsibilities between Owners and Maintainers.[189] Any federal data breach notification law should replicate California's model. California has allocated responsibilities the most efficiently by requiring that Owners notify all residents whose personal information was, or is reasonably believed to have been, acquired by an unauthorized person, while Maintainers are only required to inform the Owners.[190] This prevents inefficiencies and provides a clear separation of duties. The federal bills do not meaningfully improve on this language. By overlapping the duties of Owners and Maintainers, Congress would cause confusion, forcing Owners and Maintainers to battle over who is responsible for sending notification.[191]

In addition to requiring that notification be given to individuals, a strict federal law should also require that notification be given to both consumer reporting agencies and the Attorney General. Requiring that notification be sent to both of these entities would create a centralized place where information on data breaches could be collected and studied. In addition, it

---

[187] N.Y. GEN. BUS. LAW § 899-aa(1)(a) (McKinney 2010) (emphasis added).
[188] *See supra* note 84 and accompanying text.
[189] *See* discussion *supra* Part I.B.3.
[190] *See* CAL. CIV. CODE § 1798.82(a)–(b) (West 2010).
[191] *See supra* notes 93–95 and accompanying text.

would increase businesses' compliance with the law. Recently, California Governor Arnold Schwarzenegger vetoed a bill that would have amended California's statute to require businesses to notify the state attorney general in the event that a breach involved the information of more than 500 individuals.[192] According to the Governor, "there is no additional consumer benefit gained by requiring the Attorney General to become a repository of breach notices when this measure does not require the Attorney General to do anything with the notices."[193] Despite the Governor's objections, this requirement would put little added burden on businesses and would make the attorney general aware of possible sources of future litigation. He or she may even want to investigate particularly egregious security breaches in order to decide whether or not to prosecute. Because they will want to avoid the costs of litigation, both monetary costs and costs to their reputation, businesses faced with increased enforcement will be more likely to disclose information to the public in the event of a breach.

Notification should be delivered "in the most expedient time possible and without unreasonable delay."[194] Even though this language is vague, the bright line sixty-day deadline set forth by the House-Senate bills[195] may lead some businesses to delay notification so that they can take advantage of the full sixty days to either cover up the breach or investigate how best to notify consumers. In cases of identity theft, time is of the essence. The sooner consumers find out about the breach, the sooner they can take measures to protect their personal information. Sixty days is a lot of time for a person to wait if his or her name and credit card number has been stolen. Once again, a reviewing agency should be put in place to ensure that businesses are not delaying notification for selfish reasons. This oversight will strengthen and correct the vague language of the statute and increase consumer protection.

4. How Individuals Must Be Notified and What Information

---

[192] Nathan Taylor & Christine E. Lyon, *California Governor Vetoes Enhanced Security Breach Notification Bill*, MONDAQ, Oct. 22, 2009.

[193] *Id.*

[194] CAL. CIV. CODE § 1798.82(a).

[195] *See supra* note 112 and accompanying text.

Must Be Included in the Notification

Federal law should mandate that notification be made in writing. This medium allows businesses to give consumers a complete record of what information has been breached and where they can go for more information. The same can be said for notification by e-mail, but notification via e-mail opens individuals up to phishers. Furthermore, individuals often have numerous e-mail accounts. Often, the one that they give to businesses is one that they use for "junk e-mail." Therefore, notification via e-mail should be limited to only those circumstances in which notification in writing is not possible.

Although businesses that notify via telephone are more likely to retain the loyalty of their customers,[196] there are a number of problems with giving notice by this method. An automated telephone message cannot respond to consumer questions; the affected consumer may not be home to receive the call, causing businesses to call again and again, and there may be too much information for the consumer to write down in a short period of time. Furthermore, while opening another person's mail is a crime, there is no guarantee that the person who answers the phone is actually the person who needs to be notified. Thus, notification by telephone should not be permitted.

In addition, "substitute notification" should be an option in situations where there is no way to contact the individual or individuals involved. The Senate bills' failure to provide for substitute notification is a serious oversight because businesses left with no way to contact consumers would not be required to send notification by other means. Businesses that cannot contact the affected individuals should be required to notify state media or place a "conspicuous" posting on their websites. This will heighten the statute's " 'invisible hand' effect," whereby "each business independently looks after its own interests by imposing the level of security it believes necessary to insulate itself from liability."[197] The media can always be used as a weapon against a business's reputation.

---

[196] *See* Rode, *supra* note 152, at 1629.

[197] *Id.* at 1629–30; *see also* Raymond T. Nimmer, *Security Breach Notice Laws: Evidence?*, CONTEMPORARY INTELLECTUAL PROPERTY, LICENSING & INFORMATION LAW (Nov. 1, 2005), http://www.ipinfoblog.com/archives/privacy-data-protection-and-security-35-security-breach-notice-laws-evidence.html.

Businesses that use personalized letters are also more likely retain the loyalty of their customers;[198] thus, states were smart to specify what information must be disclosed to consumers in the event of a breach.[199] At minimum, consumers should be told: (1) what information has been breached; (2) how they can monitor their personal information; and (3) who they can contact to obtain more information. Current laws that do not require specific disclosure open the door for abuse of the law. Businesses that do not want to spend time updating their procedures to collect the information necessary for proper notification will give consumers little to no information regarding the breach, reducing consumers' ability to protect their own personal information. Specific disclosure decreases consumers' animosity and increases consumers' ability to control their personal information because consumers that know what information has been acquired have a better chance at noticing the signs of identity theft and mitigating future damages.

5. The Penalties for Failing To Notify Affected Individuals

Any federal data breach notification statute should allow for a private right of action. Fear of litigation is a strong factor in persuading businesses to comply.[200] Major data breaches lead to lawsuits, which settle even where there is no proof of negligence or harm.[201] These lawsuits can cost companies a lot of money in attorney fees, settlement agreements, and lost business. Thus it makes sense to allow lawsuits based on a failure to notify, regardless of the likelihood that such cases will succeed. Businesses will be encouraged to disclose or face the possibility of having to pay out significant sums of money, motivating them to take preventative measures by increasing investment in improved technology and security programs.

CONCLUSION

A uniform data breach notification law that preempts the forty-six state laws currently in place would end many of the difficulties faced by businesses engaged in interstate commerce, while increasing consumers' control over their own personal

---

[198] *See* Rode, *supra* note 152, at 1629.
[199] *See* discussion *supra* Part I.B.4.
[200] Picanso, *supra* note 153, at 373.
[201] Danzig et al., *supra* note 1, at 61.

information. The law enacted must be strict. It must increase the chances that businesses will disclose information to the public in the most expedient time possible in the event of a breach. A federal data breach notification statute with language that provides for an acquisition based trigger, a broad definition of personal information and a private right of action will strengthen the incentives for businesses to invest in security and implement improved data protection procedures. Furthermore, a federal agency should be put in charge of overseeing businesses' determinations regarding whether a security breach has taken place and when notification is required. The media, the U.S. Attorney General, and the new federal agency should all play a role in enforcing the law. Residents of Alabama, Kentucky, New Mexico, and South Dakota should no longer have to wait for their states to provide them with the same protections that other residents of the United States currently enjoy. Until Congress passes a federal data breach notification law, consumers in the United States will remain unprotected, while businesses bear the costs of a complicated state statutory scheme.