

The Data Game: Learning to Love the State-Based Approach to Data Breach Notification Law*

INTRODUCTION	267
I. DATA BREACH NOTIFICATION LAWS.....	272
A. <i>The Anatomy of a Data Breach Notification Law</i>	273
1. Personally Identifiable Information.....	275
2. Scope of Statute	277
3. Form and Timing of Notice.....	279
B. <i>Interests Protected: What Interest Is Really at the Heart of Data Breach Notification Laws?</i>	280
1. Data Control: Financial Interests.....	281
2. Information Privacy: Dignitary Interests.....	284
C. <i>Reconciling the Interests</i>	287
II. STATE-BASED APPROACHES	287
A. <i>State Laws Are Tailored to Protect Specific Interests</i>	288
B. <i>State Laws Are Already Supplemented by Federal, Industry-Specific Laws</i>	293
III. THE FEDERAL PROPOSALS	297
A. <i>Arguments for a Federal Standard</i>	298
B. <i>A Survey of Key Bills Pending in Congress</i>	299
IV. WHY A FEDERAL LAW IS NOT THE SOLUTION	301
A. <i>Federalism and Market-Based Equilibrium</i>	302
B. <i>Preemption</i>	306
C. <i>Inflexibility</i>	308
CONCLUSION.....	308

INTRODUCTION

You give it away all the time. You trade it for discounts at grocery stores. You offer it in exchange for the convenience of making purchases and banking online. You even allow universities to store it so that they can come collecting during alumni fund drives. Packets of data identifying you—as an individual—are stored, sold, and swapped in more forums than it is possible to account for.¹ The

* © 2009 Sara A. Needles.

1. Indeed, more than once this author provided her name, address, e-mail address, telephone number, and organizational affiliation via Web site form in order to access materials for use in this Comment. See Nicholas A. Lassow & Jamie Ourada, *Personal Information: A New Currency of Exchange*, in TECHNOLOGY AND PRIVACY IN THE NEW MILLENNIUM 50, 50–59 (Kai R. Larsen & Zoya A. Voronovich eds., 2004) (discussing the

digitized data can be transferred from server to server, from server to hard drive, or from hard drive to USB memory stick with all the ease of copying an electronic file.² And then comes the letter or e-mail or phone call with the news that some of these packets of data, including yours, may have been accessed by prying eyes.³ Often the organization responsible for securing the data does not even know who compromised the information or for what purpose.⁴

The torrent of such messages is partly a result of the proliferation of state data breach notification laws that began in 2003.⁵ As headlines signal more breaches, increasing attention is being paid to the security of individuals' personal information, particularly when that data is digitized. A swell that analysts once explained as the result of more widespread disclosure obligations now seems to

frequency with which people trade their personal details for perks); Thomas J. Smedinghoff, *The Emerging Law of Data Security: A Focus on the Key Legal Trends*, in 1 NINTH ANNUAL INSTITUTE ON PRIVACY AND SECURITY LAW, at 13, 19 (PLI Intellectual Prop., Course Handbook Series No. 934, 2008) (“[I]n today’s business environment, virtually all of a company’s daily transactions and all of its key records are created, used, communicated, and stored in electronic form using networked computer technology.”).

2. See, e.g., SERGE GUTWIRTH, *PRIVACY AND THE INFORMATION AGE* 61 (Raf Casert trans., Rowman & Littlefield Publishers 2002) (1998) (“Information technology has enabled the lightning-fast, efficient, delocalized, and omnipresent processing of enormous amounts of personal information. It has made individuals and their behavior transparent, retraceable, and controllable.”).

3. See Liisa M. Thomas, *The Emerging Law of Data Security: From Corporate Obligations to Provide Security to Breach Notification Requirements*, in 1 NINTH ANNUAL INSTITUTE ON PRIVACY AND SECURITY LAW, at 357, 368 (PLI Intellectual Prop., Course Handbook Series No. 934, 2008) (“The primary purpose of these laws is to ensure that businesses notify consumers and employees when their personal data has been breached.”).

4. See, e.g., Thomas Claburn, *Heartland Payment Systems Hit by Security Breach*, INFORMATIONWEEK, Jan. 20, 2009, <http://www.informationweek.com/news/security/attacks/showArticle.jhtml?articleID=212901505> (“We don’t know in what way there was egress or to what extent. . . . [W]e don’t know the percentage of transactions that the sniffer was able to grab. And we don’t know the percentage of those that the bad guys were able to access.”).

5. Since 2003 forty-five states, Washington, D.C., Puerto Rico, and the U.S. Virgin Islands have enacted breach notification laws. National Conference of State Legislatures, *State Security Breach Notification Laws*, <http://www.ncsl.org/programs/lis/cip/priv/breachlaws.htm> (last visited Oct. 28, 2009) (listing the notification laws); see also John B. Kennedy & Anne E. Kennedy, *What Went Wrong? What Went Right? Corporate Responses to Privacy and Security Breaches*, in 2 EIGHTH ANNUAL INSTITUTE ON PRIVACY AND SECURITY LAW: PATHWAYS TO COMPLIANCE IN A GLOBAL REGULATORY MAZE, at 11, 19 (PLI Intellectual Prop., Course Handbook Series No. 903, 2007) (2007) (“[T]he first such state law [was] adopted by California in 2003.”). The general mechanism behind these statutes is that a company that encounters unauthorized access to records that include an individual’s name plus social security number, driver’s license number, or financial account details must disclose the breach to affected individuals. See *infra* Part I.A.

indicate that the actual number of breaches is on the rise.⁶ The public has also been paying attention because, until recently, consumer costs in the wake of a breach were also on the rise.⁷

In response to the surge of data breaches, and as mass data storage becomes increasingly mobile and thus susceptible to loss or theft, states and federal agencies have enacted laws and promulgated rules to respond to and stanch security breaches.⁸ Because businesses often operate in multiple states and because of the overlap between state laws and sector-specific requirements—such as the Gramm-Leach-Bliley Act,⁹ the Fair and Accurate Credit Transactions Act,¹⁰

6. See Brian Krebs, *Data Breaches Are Up 69% This Year, Nonprofit Says*, WASH. POST, July 1, 2008, at D3 (discussing the difficulty of analyzing whether the jump in figures reflects an increase in actual incidents, an increase in reporting, or both). According to the Identity Theft Resource Center, there were 656 reported breaches in 2008, compared with 446 in 2007, 315 in 2006, and 158 in 2005. See IDENTITY THEFT RES. CTR., ITRC BREACH REPORT 2008, at 1 (2008), http://www.idtheftcenter.org/artman2/uploads/1/ITRC_Breach_Report_2008_final_1.pdf; IDENTITY THEFT RES. CTR., ITRC BREACH REPORT 2007, at 1 (2007), http://www.idtheftcenter.org/artman2/uploads/1/ITRC_Breach_Report_20071231_1.pdf; IDENTITY THEFT RES. CTR., ITRC BREACH REPORT 2006, at 1 (2006), http://www.idtheftcenter.org/artman2/uploads/1/ITRC_Breach_Report_20061231.pdf; IDENTITY THEFT RES. CTR., ITRC BREACH REPORT 2005, at 1 (2005), http://www.idtheftcenter.org/artman2/uploads/1/ITRC_Breach_Report_20051231_1.pdf. The Identity Theft Res. Ctr. also provides a running total of data breaches. Identity Theft Resource Center, <http://www.idtheftcenter.org/index.html> (last visited Nov. 18, 2009) (follow “Data Breaches” navigation button). For a discussion of the increasing threat from employee behaviors, see CISCO, DATA LEAKAGE WORLDWIDE: THE HIGH COST OF INSIDER THREATS (2008), http://www.cisco.com/en/US/solutions/collateral/ns170/ns896/ns895/white_paper_c11-506224.pdf.

7. Compare PONEMON INST., 2007 ANNUAL STUDY: U.S. COST OF A DATA BREACH 2 (2007), http://download.pgp.com/pdfs/Ponemon_COB-2007_US_071127_F.pdf (analyzing the actual costs thirty-five organizations incurred when responding to data breach incidents that resulted in the loss or theft of protected personal information), with Candice Choi, *Survey: Identity Theft Up, but Costs Fall Sharply*, ABC NEWS, Feb. 9, 2009, <http://abcnews.go.com/Business/wireStory?id=6833833> (reporting that the consumer cost per incident fell thirty-one percent in 2008).

8. While this Comment focuses on U.S. law, there are also international agencies and treaties at work in the data security arena. See, e.g., Council Directive 95/46, 1995 O.J. (L 281) 1 (regulating data processing and storage within the European Union); JOINT TECHNICAL COMM. OF THE INT’L ORG. FOR STANDARDIZATION AND THE INT’L ELECTROTECHNICAL COMM’N, INFORMATION TECHNOLOGY—SECURITY TECHNIQUES—CODE OF PRACTICE FOR INFORMATION SECURITY MANAGEMENT, ISO/IEC (2005) (providing best practices for information technology systems managers for the confidentiality, integrity, and availability of data); ORG. FOR ECON. CO-OPERATION AND DEV., OECD GUIDELINES ON THE PROTECTION OF PRIVACY AND THE TRANSBORDER FLOWS OF PERSONAL DATA (2002), http://www.oecd.org/document/18/0,2340,en_2649_34255_1815186_1_1_1_1,00.html (setting forth data privacy guidelines for industry and governments that enable the transborder transfer of information).

9. Gramm-Leach-Bliley Financial Modernization Act, Pub. L. No. 106-102, 113 Stat. 1338 (1999) (codified as amended in scattered sections of 12, 15, and 16 U.S.C.).

and the Health Insurance Portability and Accountability Act¹¹—they may need to comply with several sets of laws. This multiplicity of legislative layers has led to calls for a consistent federal standard that would supersede state laws, creating a comprehensive, uniform law.¹² Supporters of a federal breach notification law argue that a single, one-size-fits-all notification statute will ease the compliance burden for companies and provide needed protection to consumers.¹³ The focus of the data breach debate at the federal level has largely been on identity theft and the financial harm that flows from it.¹⁴ But state legislators have enacted breach notification laws to protect a variety of interests.¹⁵ More than simply combating identity theft and economic harm to individuals, many state data breach notification

10. Fair and Accurate Credit Transactions Act (FACTA) of 2003, Pub. L. No. 108-159, 117 Stat. 1952 (codified as amended in scattered sections of 15 U.S.C.) (amending the Fair Credit Reporting Act of 1970, Pub. L. No. 91-508, 84 Stat. 1114 (codified as amended at 15 U.S.C. §§ 1681–1681x)).

11. Health Insurance Portability and Accountability Act (HIPAA) of 1996, Pub. L. No. 104-191, 110 Stat. 1936 (codified as amended in scattered sections of 18, 26, 29, and 42 U.S.C.). The privacy regulations are codified at 45 C.F.R. pts. 160, 164 (2008 & Supp. 2009).

12. See, e.g., Posting of Arianna to Laptop Security Blog, *Bill Gates Encourages Federal Privacy Law*, <http://blog.absolute.com/bill-gates-encourages-federal-privacy-law/> (Mar. 21, 2007) (“Gates, and other companies and lobbyists, are encouraging a privacy law at the federal level to overcome the disparate and uneven state security laws.”); CTR. FOR STRATEGIC AND INT’L STUDIES, *SECURING CYBERSPACE FOR THE 44TH PRESIDENCY* 43, 49 (2008), http://csis.org/files/media/csis/pubs/081208_securingcyberspace_44.pdf (discussing the need for governmental cooperation with industry and private citizens to secure data as well as the need for a common security standard across industries); Robert Westervelt, *Group Gives Government Low Marks on Data Protection*, SEARCHSECURITY.COM, Jan. 31, 2007, http://searchsecurity.techtarget.com/news/article/0,289142,sid14_gci1241644,00.html (citing Cyber Security Industry Alliance’s report “criticizing Congress for failing to pass a comprehensive data security law in 2006”).

13. See Declan McCullagh, *Security Breach Laws Become State’s Rights Issue*, CNET NEWS, Apr. 13, 2005, http://news.cnet.com/Security-breach-laws-become-states-rights-issue/2100-7348_3-5669991.html (“Acxiom supports efforts to pass federal pre-emptive legislation requiring notice to consumers in the event of a security breach, where such breach places consumers at risk of identity theft or fraud.” (quoting Acxiom chief privacy officer Jennifer Barrett)).

14. See, e.g., CONG. RESEARCH SERV., *REPORT FOR 111TH CONG., FEDERAL INFORMATION SECURITY AND DATA BREACH NOTIFICATION LAWS 2* (2009), <http://fas.org/sgp/crs/secretcy/RL34120.pdf> (“Data breaches involving sensitive personal information may result in identity theft and financial crimes (e.g., credit card fraud, phone or utilities fraud, bank fraud, mortgage fraud, employment-related fraud, government documents or benefits fraud, loan fraud, and health-care fraud).”).

15. See Anupam Chander, *Introduction: Securing Privacy in the Internet Age*, in *SECURING PRIVACY IN THE INTERNET AGE* 1, 5 (Anupam Chander, Lauren Gelman & Margaret Jane Radin eds., 2008) (“Privacy and security are not the only values in designing an information regime. There are many other values, including innovation; efficient production and distribution; access to cheaper goods and services . . . ; simplicity; functionality; and free speech.”).

laws strike a balance between the conflicting effects on consumers and businesses.¹⁶ Analyzing what a breach notification portends implicates these two main parties that, in terms of privacy interests, are at odds with one another. Business interests in monetizing data clash against consumer protection groups' cry for data privacy.¹⁷

This Comment rejects the notion that a comprehensive federal standard is the best way to protect the interests served by data breach notification laws. Part I draws the contours of a data breach law and examines the different interests that notification laws seek to protect. Breach notification laws encompass measurable, economic injuries stemming from loss of control over data (typically understood in terms of identity theft) as well as injuries that are intangible yet still represent a violation of information privacy.¹⁸ Understanding this tension between financial "data control" on the one hand and dignitary "information privacy" on the other is the key to identifying the consumer interests at the heart of breach laws.¹⁹ Only by identifying these two types of consumer interests, and then weighing those interests against business interests, can notification laws be evaluated. Part II examines the state of the law, evaluating the ways in which states have weighed the financial and dignitary harms to consumers laid out in Part I against protecting business interests in their jurisdictions. Truly regulable data processes, such as how credit card information is collected and stored, have generated federal, industry-specific laws to cover the essentials of data breach notification from a consumer perspective. Part III introduces the range of federal proposals for a uniform notification standard, highlighting provisions that would affect the current patchwork regime. Part IV argues that a federal law is not the best solution

16. See, e.g., Joan Goodchild, *Federal Breach Law? No Time Soon*, NETWORK WORLD, Dec. 11, 2008, <http://www.networkworld.com/news/2008/121108-federal-breach-law-no-time.html> (explaining that businesses want a high threshold before notification is required, while consumers believe that giving businesses discretion will leave them unprotected).

17. See, e.g., Judi Hasson, *Don't Expect a Federal Anti-Breach Law*, FIERCECIO, Dec. 13, 2008, <http://www.fiercecio.com/story/dont-expect-federal-anti-breach-law/2008-12-13> ("Chris Wolf, a Washington, D.C., attorney with Proskauer Rose LLP and chair of its privacy and security practice group, said the battle lines have been drawn between business interests and consumers [sic] groups, making a compromise unlikely.").

18. Edward J. Janger & Paul M. Schwartz, *Anonymous Disclosure of Security Breaches*, in SECURING PRIVACY IN THE INTERNET AGE, *supra* note 15, at 223, 231; see *infra* Part I.B.

19. See, e.g., Lilia Rode, Comment, *Database Security Breach Notification Statutes: Does Placing the Responsibility on the True Victim Increase Data Security?*, 43 Hous. L. Rev. 1597, 1606 (2007) ("Privacy and data protection exist as separate and distinct concepts supported by different public policy concerns.").

because it would weaken states' abilities to protect those interests that they value most. Principles of federalism, preemption, and the inflexibility of federal law expose the feebleness of a federal approach for data protection. This Comment concludes that state statutes—combined with subject area specific, federal regulations—are more discerning tools for data security policy than a blunt federal standard.

I. DATA BREACH NOTIFICATION LAWS

When an unauthorized person breaches a database containing “personally identifiable information,” state or federal law may require the entity maintaining the database to notify the affected individuals.²⁰ Security breach notification laws are designed to put consumers on notice that their personal information has been compromised,²¹ allowing individuals to take the action they feel is necessary to protect themselves. Depending on the type of information compromised, the individual may choose to respond in various ways depending on the degree to which he feels at risk from the breach.²² The idea is that by requiring companies to disclose a breach, the laws generate public awareness, which in turn encourages consumer vigilance.

So far, the value of data breach notification laws is difficult to quantify because compliance is often conflated with effectiveness.²³ The notification provisions' purpose is to inform individuals of a

20. See, e.g., Samuel Lee, Comment, *Breach Notification Laws: Notification Requirements and Data Safeguarding Now Apply to Everyone, Including Entrepreneurs*, 1 ENTREPRENEURIAL BUS. L.J. 125, 130–31 (2006) (explaining that the scope of statutory notification requirements depends on variables including the type of data covered, format and timing of notice, and applicability of exceptions).

21. See *supra* note 3 and accompanying text.

22. For example, an individual learning that her telephone number, social security number, or bank account details have been compromised might variably choose to engage a credit monitoring service, obtain new account numbers, or do nothing.

23. See James T. Graves, Note, *Minnesota's PCI Law: A Small Step on the Path to a Statutory Duty of Data Security Due Care*, 34 WM. MITCHELL L. REV. 1115, 1116 (2008) (arguing that while breach notification laws have increased awareness of the issue, they have not improved the initial problem of inadequate security); Kathryn E. Picanso, Comment, *Protecting Information Security Under a Uniform Data Breach Notification Law*, 75 FORDHAM L. REV. 355, 373 (2006) (suggesting that while some security measures are more robust as a result of compliance, the percentage of companies that comply is low); Ben Worthen, *New Data Privacy Laws Set for Firms*, WALL ST. J., Oct. 16, 2008, at B1 (emphasizing that data breach notification laws differ from data security laws and that breach notification laws have done little nationwide to reduce security breaches). *But see* Thomas Oscherwitz, *Short Shelf Life for Data Breach Laws?*, CNET NEWS, Mar. 2, 2006, http://news.cnet.com/Short-shelf-life-for-data-breach-laws/2010-7348_3-6044865.html (“Data-breach laws have had a remarkable and positive effect on security practices in the United States.”).

breach—that is all.²⁴ But who should bear the cost of a breach? As the true perpetrators of security breaches operate under the cloak of anonymity, it is difficult to place cost, let alone blame, on the breacher.²⁵ While companies responsible for databases of personally identifiable information are rapidly learning that it is in their interest to prevent breaches,²⁶ the notification laws themselves only incidentally bring about this effect.²⁷ In addition, analyzing the effectiveness of data breach notification laws is complicated by companies' individual efforts at developing a privacy policy that may recognize even more responsibility than state statutes require.²⁸ Despite their uncertain utility, however, state notification laws, supplemented by a few important federal, industry-specific standards, set the tone for how the stakeholders involved in a data breach interact.

A. *The Anatomy of a Data Breach Notification Law*

The working definition of “data breach” for this Comment will be “the unauthorized access of computerized data that compromises

24. Dennis Fisher, *Data Breach Laws Have No Effect on Prevention, Researchers Say*, SEARCHSECURITY.COM, June 9, 2008, http://searchsecurity.techtarget.com/news/article/0,289142,sid14_gci1316837,00.html (“The onus is on the consumer to take action . . . They feel overconfident that it won’t happen to them, and the odds are that they’re right. There’s inertia . . . and a lack of understanding to properly perceive what the consequences might be.” (internal quotations omitted) (quoting Sasha Romanosky, a Ph.D. student at Carnegie Mellon University studying data breaches)).

25. Daniel J. Solove, *The New Vulnerability: Data Security and Personal Information*, in SECURING PRIVACY IN THE INTERNET AGE, *supra* note 15, at 111, 115 (“Identity thieves are difficult to catch. An identity theft often occurs in many different locations, and law enforcement officials ‘sometimes tend to view identity theft as being “someone else’s problem.”’” (quoting U.S. GEN. ACCOUNTING OFFICE, REPORT TO THE HONORABLE SAM JOHNSON, HOUSE OF REPRESENTATIVES, IDENTITY THEFT: GREATER AWARENESS AND USE OF EXISTING DATA ARE NEEDED 18 (2002))). Most cases of identity theft are never solved. *Id.* (“[Fewer than] one in seven hundred instances of identity theft result in a conviction.”).

26. Bill Brenner, *Should TJX Really Be Worried About Data Breach Fallout?*, SEARCHSECURITY.COM, Oct. 24, 2007, http://searchsecurity.techtarget.com/news/article/0,289142,sid14_gci1278757,00.html (noting that heightened awareness of data breaches is increasing businesses’ attention to security policies).

27. Fisher, *supra* note 24 (“Some of the reasoning for passing breach notification laws is that putting these incidents in the public eye will force companies to be more careful with their security practices, which will theoretically result in fewer breaches in the future.”).

28. See Smedinghoff, *supra* note 1, at 23 (discussing companies’ representations regarding data security through privacy policy statements, Web sites, or marketing materials). “By making such statements, companies impose on themselves an obligation to comply with the standard they have represented to the public that they meet.” *Id.*

the security, confidentiality, or integrity of personal information.”²⁹ Thus, a data breach can take the shape of a lost or stolen laptop or USB drive, an individual unintentionally misusing data, employee espionage, a vendor inappropriately authorizing use of data, or an external intrusion (i.e., hacking).³⁰ Research suggests that the cause of data breaches and the technological environment where data breaches occur are linked; for example, off-network, mobile devices are more vulnerable than mainframes,³¹ with lost or stolen devices being the most likely root of compromised information.³² The Bureau of Alcohol, Tobacco, Firearms, and Explosives illustrated a typical data loss scenario when they lost hundreds of laptops between 2002 and 2007—many containing classified or sensitive data.³³ In 2008 companies and organizations such as the Federal Emergency Management Agency, Hewlett-Packard, Starbucks, Shell Oil, BlueCross and BlueShield, and more than sixty colleges and universities reported data breaches owing to the loss or theft of

29. Thomas, *supra* note 3, at 368. This language closely tracks definitions used in many states, including California. CAL. CIV. CODE § 1798.82 (West 2009). The main variation on this definition has to do with some states’ extension of data breaches to hard-copy material in addition to electronic data. *E.g.*, IND. CODE ANN. § 24-4.9-2-2 (LexisNexis 2006) (“ ‘Breach of the security of a system’ . . . 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.”); N.C. GEN. STAT. § 75-65 (2007) (covering personal information “in any form (whether computerized, paper, or otherwise)”). The Identity Theft Resource Center and the Privacy Rights Clearinghouse use “security breach.” *See* Identity Theft Res. Ctr., Data Breaches, http://www.idtheftcenter.org/artman2/publish/lib_survey/ITRC_2008_Breach_List.shtml (last visited Nov. 7, 2009) (using the terms “security breach” and “data breach”); Privacy Rights Clearinghouse, Fact Sheet 17(b): Security Breach Guide, <http://www.privacyrights.org/fs/fs17b-SecurityBreach.htm> (last visited Nov. 7, 2009) (using the term “security breach”). The more vivid “data spill” analogizes to an oil spill, where some pieces of information cling to the shore for anyone to stumble upon and other pieces float on a vast ocean, not easily obtainable but nevertheless there, indefinitely. *See* Jack Schoefield, *Newly Asked Questions: Has the Time Come to Stop Using Google?*, THE GUARDIAN, Aug. 17, 2006, (Technology Guardian), at 2, available at <http://www.guardian.co.uk/technology/2006/aug/17/guardianweeklytechnologysection.google> (dubbing AOL’s “data spill” a “data Valdez”).

30. *See* Eduard F. Goodman, *Your Duty If You Discover a Data Breach*, GPSOLO, Dec. 2008, at 16, 17.

31. PONEMON INST., 2008 STUDY ON THE UNCERTAINTY OF DATA BREACH DETECTION 4–5 (2008), <http://www.ponemon.org/local/upload/fckjail/generalcontent/18/file/2008%20US%20Uncertainty%20of%20Data%20Breach%20Detection%20Final%20June%202008.pdf>.

32. *See* Krebs, *supra* note 6.

33. Holly Watt, *ATF Lost Guns, Computers*, WASH. POST, Sept. 18, 2008, at A19. The Bureau of Alcohol, Tobacco, Firearms and Explosives did not have records of the information that was stored on many of the devices. *Id.*

personal information, including social security numbers.³⁴ The estimated (that is, reported) number of records affected from all breaches since January 2005 is a staggering 340,097,773.³⁵ Whether or not unauthorized access in any of these cases triggers a duty to notify depends on three key variables in state notification laws: the statute's definition of "personally identifiable information," the statute's scope and whether it includes a risk-based exemption, and the form and timing of notice the statute prescribes.

1. Personally Identifiable Information

To determine when unauthorized access of personal information triggers an obligation to notify those individuals identified by the data, current state laws define what is considered to be "personally identifiable information" for the purposes of the notification laws.³⁶ The definition chosen by each state reflects the interests at the heart of each state's law.³⁷ California's breach notification law—the first state notification statute enacted in the United States—defines personal information as

[an] individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted:

- (1) Social security number.
- (2) Driver's license number or California Identification Card number.
- (3) Account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.

34. Privacy Rights Clearinghouse, A Chronology of Data Breaches, <http://www.privacyrights.org/ar/ChronDataBreaches.htm#CP> (last visited Nov. 19, 2009).

35. *Id.* This number does *not* include records in which an individual's social security number or financial account information was not revealed and only reflects records breached through October 15, 2009. *Id.*

36. Thomas M. Laudise, *Ten Practical Things to Know About "Sensitive" Data Collection and Protection*, in INFORMATION TECHNOLOGY LAW INSTITUTE 2008: NEW DIRECTIONS; SOCIAL NETWORKS, BLOGS, PRIVACY, MASH-UPS, VIRTUAL WORLDS AND OPEN SOURCE, at 389, 399 (PLI Intellectual Prop., Course Handbook Series No. 929, 2008).

37. *See infra* Parts I.B, II.A.

(4) Medical information.

(5) Health insurance information.³⁸

California is somewhat unusual in including health information, as many states restrict the scope of personally identifiable information to just the first three elements in the California statute.³⁹ Other state laws include an individual's alien registration number, passport number, date of birth, digitized or electronic signature, medical records, biometric data, DNA profile, tax information, work evaluations, or mother's maiden name as additional data elements that can trigger a breach.⁴⁰ A broader, more holistic definition of sensitive data would extend to any "information which a customer would not feel comfortable being in the hands of an unauthorized third party."⁴¹ To mitigate a potentially overinclusive definition of

38. CAL. CIV. CODE § 1798.29 (West 2009). California's security breach notification law, popularly referred to by its original bill number (S.B. 1386), was enacted in 2003 and serves as the model for many other states' statutes. Lee, *supra* note 20, at 131.

39. See, e.g., CONN. GEN. STAT. ANN. § 36a-701b(a) (West Supp. 2009) (" '[P]ersonal information' means an individual's first name or first initial and last name in combination with any one, or more, of the following data: (1) Social Security number; (2) driver's license number or state identification card number; or (3) account number, credit or debit card number, in combination with any required security code, access code or password that would permit access to an individual's financial account."); see also FLA. STAT. ANN. § 817.5681(5) (West 2006) (" '[P]ersonal information' means an individual's first name, first initial and last name, or any middle name and last name, in combination with any one or more of the following data elements when the data elements are not encrypted: (a) Social security number. (b) Driver's license number or Florida Identification Card number. (c) Account number, credit card number, or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account."); MASS. ANN. LAWS ch. 93H, § 1(a) (LexisNexis Supp. 2009) (" 'Personal information' [is] a resident's first name and last name or first initial and last name in combination with any 1 or more of the following data elements that relate to such resident: (a) Social Security number; (b) driver's license number or state-issued identification card number; or (c) financial account number, or credit or debit card number, with or without any required security code, access code, personal identification number or password, that would permit access to a resident's financial account.").

40. Ian C. Ballon, *A Legal Analysis of State Security Breach Statutes*, in 2 EIGHTH ANNUAL INSTITUTE ON PRIVACY AND SECURITY LAW: PATHWAYS TO COMPLIANCE IN A GLOBAL REGULATORY MAZE, at 135, 142-44 (PLI Intellectual Prop., Course Handbook Series No. 903, 2007) (collecting statutes that include these more expansive elements); Goodman, *supra* note 30, at 17; Alan S. Wernick, *Data Theft and State Law*, J. AHIMA, Nov.-Dec. 2006, at 40, 41, available at http://www.privacyrights.org/ar/Wernick_Dec06.pdf (listing data elements that may be considered personally identifiable information under state law).

41. Laudise, *supra* note 36, at 399 (noting that while no state uses this exact formulation, entities ought to treat as personally identifiable information any data that could be used to commit a fraud). Depending on whether a state chooses this sort of definition, data arising from behavioral marketing that has been sold or otherwise breached could also come within the statute's scope. See GUTWIRTH, *supra* note 2, at 2

personally identifiable information, a statute might carve out an exception for publicly available information that has been lawfully provided to the general public from government records.⁴²

2. Scope of Statute

A state's statute will specify to whom the notification obligation applies. For example, California's law applies to a "person or business that conducts business in California, and that owns or licenses computerized data that includes personal information."⁴³ Other states' statutes may be broader or narrower: Delaware's breach law extends to individuals and commercial entities,⁴⁴ while Oklahoma's law applies only to "any state agency, board, commission or other unit . . . of state government that owns or licenses computerized data that includes personal information."⁴⁵ Georgia's law applies only to information brokers and data collectors.⁴⁶

The statute also may specify at what point an entity's duty to notify those individuals whose data has been compromised is

("[P]rivacy is often defined as the control of individuals over what happens with their personal information.")

42. *See, e.g.*, CAL. CIV. CODE § 1798.82(f)(1) (West 2009) (" '[P]ersonal information' does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records."); N.C. GEN. STAT. § 75-61(10) (2007) ("Personal information does not include publicly available directories containing information an individual has voluntarily consented to have publicly disseminated or listed . . ."); *see also* MASS. ANN. LAWS ch. 93H, § 1(a) (LexisNexis Supp. 2009) (" 'Personal Information' shall not include information that is lawfully obtained from publicly available information, or from federal, state or local government records lawfully made available to the general public."); WASH. REV. CODE ANN. § 19.255.010(5) (West 2007) (providing exceptions similar to California's).

43. CAL. CIV. CODE § 1798.82(a) (West 2009).

44. DEL. CODE ANN. tit. 6, § 12B-101 (2005) (limiting this more inclusive scope by requiring that the unauthorized acquisition compromise "the security, confidentiality, or integrity of personal information").

45. OKLA. STAT. ANN. tit. 74, § 3113.1(A) (West Supp. 2009).

46. GA. CODE ANN. § 10-1-911(1) (2009). Georgia's law defines information broker as

any person or entity who, for monetary fees or dues, engages in whole or in part . . . in the business of collecting, assembling, evaluating, compiling, reporting, transmitting, transferring, or communicating information concerning individuals for the primary purpose of furnishing personal information to nonaffiliated third parties, but does not include any governmental agency whose records are maintained primarily for traffic safety, law enforcement, or licensing purposes.

§ 10-1-911(3). A data collector is "any state or local agency or subdivision thereof including any department, bureau, authority, public university or college, academy, commission, or other government entity." § 10-1-911(2).

triggered.⁴⁷ California's law is triggered when there is a reasonable belief that sensitive, personal information has been acquired or accessed by an unauthorized person.⁴⁸ In Kansas, notification is required where the breached entity reasonably believes that the breach "has caused or will cause[] identity theft to any consumer,"⁴⁹ whereas in Rhode Island, disclosure is required upon "any breach of the security of the system which poses a significant risk of identity theft."⁵⁰ Even if the type of data that is unlawfully accessed falls within a statute's definition of personally identifiable information and satisfies a trigger, a further threshold criterion may need to be met: some statutes require there to be a likelihood that information will be misused⁵¹ or that the breach be material.⁵² This is generally referred to as a "risk-based exemption."⁵³ Notification requirements may also depend on the type of medium compromised: some states' laws apply to both computerized and hard-copy breaches,⁵⁴ while others cover only computerized data.⁵⁵ Most states exclude encrypted or password-protected data, providing a sort of safe harbor against an obligation to

47. See Ballon, *supra* note 40, at 139 ("Whether a breach requiring notice has occurred may depend on applicable state law or regulation.").

48. CAL. CIV. CODE § 1798.82(a) (West 2009).

49. Ballon, *supra* note 40, at 141 (quoting KAN. STAT. ANN. § 50-7a01(h) (2006)).

50. *Id.* (citing R.I. GEN. LAWS § 11-49.2-3 (Supp. 2008)).

51. See Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice, 70 Fed. Reg. 15,736, 15,741 (Mar. 29, 2005).

52. Ballon, *supra* note 40, at 144-45. The definition of "materiality" differs from statute to statute. Compare FLA. STAT. ANN. § 817.5681(10)(a) (West 2006) ("[N]otification is not required if, after an appropriate investigation or after consultation with relevant federal, state, and local agencies responsible for law enforcement, the person reasonably determines that the breach has not and will not likely result in harm to the individuals whose personal information has been acquired and accessed."), and ARK. CODE ANN. § 4-110-105(d) (Supp. 2009) ("Notification under this section is not required if, after a reasonable investigation, the person or business determines that there is no reasonable likelihood of harm to customers."), and WIS. STAT. ANN. § 134.98 (West 2008) ("[A]n entity is not required to provide notice of the acquisition of personal information if . . . [t]he acquisition of personal information does not create a material risk of identity theft or fraud to the subject of the personal information."), with WASH. REV. CODE ANN. § 19.255.010(4) (West 2007) ("'[B]reach of the security of the system' means unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the person or business.").

53. David L. Silverman, *Data Security Breaches: The State of Notification Laws*, 19 INTELL. PROP. & TECH. L.J. 5, 6 (2007).

54. See, e.g., MASS. LAWS ANN. ch. 93H, § 1(a) (LexisNexis Supp. 2009).

55. See, e.g., IDAHO CODE ANN. § 28-51-105(1) (Supp. 2009) ("An agency, individual or a commercial entity that conducts business in Idaho and that owns or licenses computerized data that includes personal information about a resident of Idaho shall, when it becomes aware of a breach of the security of the system, conduct in good faith a reasonable and prompt investigation to determine the likelihood that personal information has been or will be misused.").

notify so long as the encryption key or password has not also been compromised.⁵⁶

3. Form and Timing of Notice

If a breach triggers disclosure, the notice must follow the applicable state statute's form and content requirements. Most states require that the entity sustaining the breach disclose the breach via hard-copy mail or e-mail but do not specify the exact content that the notice must contain.⁵⁷ Some states require that notice include details regarding the type of information breached, the scope of the incident, and the availability of free credit reports.⁵⁸ State laws may provide for exceptions to a general notification requirement where the cost of notification exceeds a certain threshold.⁵⁹ They may also permit alternative means of notification (such as telephone call,⁶⁰ newspaper publication,⁶¹ or media release⁶²) or may require disclosure to third parties, such as credit reporting agencies, credit bureaus, or state agencies.⁶³ Many states require that notification occur as soon as

56. Goodman, *supra* note 30, at 17. Wyoming does not provide an exemption for encrypted data. WYO. STAT. ANN. § 40-12-502 (2009).

57. Paul J. Siegel, *Responding to an Unauthorized Breach of Electronic Personal Information*, INT'L RISK MGMT. INST., Nov. 2006, <http://www.irmi.com/Expert/Articles/2006/Siegel11.aspx>. However, some states do provide detailed content requirements. Hawaii mandates a notice that is "clear and conspicuous" and contains specific information: description of the breach, types of data compromised, company's responding efforts to resecure the information, a telephone number to call for further information, and advice instructing the individual to monitor account statements and credit reports for accuracy. *Id.*

58. *Id.* For a representative statute of this nature, see N.H. REV. STAT. ANN. § 359-C:20(IV) (LexisNexis 2008) ("Notice under this section shall include at a minimum: (a) A description of the incident in general terms. (b) The approximate date of breach. (c) The type of personal information obtained as a result of the security breach. (d) The telephonic contact information of the person subject to this section.").

59. *See, e.g.*, KAN. STAT. ANN. § 50-7a01(c)(3) (Supp. 2008) (" 'Notice' means . . . substitute notice[] if the individual or the commercial entity required to provide notice demonstrates that the cost of providing notice will exceed \$100,000, or that the affected class of consumers to be notified exceeds 5,000, or that the individual or the commercial entity does not have sufficient contact information to provide notice").

60. States including Connecticut, Montana, New York, and North Carolina permit telephone disclosure. CONN. GEN. STAT. ANN. § 36a-701b(e) (West Supp. 2009); MONT. CODE ANN. § 30-14-1704(5)(a)(iii) (2009); N.Y. GEN. BUS. LAW § 899-aa(5)(c) (McKinney 2005); N.C. GEN. STAT. § 75-65(e)(3) (2007).

61. *E.g.*, UTAH CODE ANN. § 13-44-202(5)(a)(iv)(A) (Supp. 2009).

62. *E.g.*, N.H. REV. STAT. ANN. § 359-C:20(III)(d)(3) (LexisNexis 2008).

63. Krebs, *supra* note 6 (stating that Maryland, New Hampshire, and Wisconsin require that data breaches be reported to state officials).

reasonably possible,⁶⁴ but some states, like Texas, permit delay in order to cooperate with law enforcement investigations.⁶⁵

B. Interests Protected: What Interest Is Really at the Heart of Data Breach Notification Laws?

Just as with other aspects of public policy, states design data protection policy in accordance with the particular balance of interests and values in a given state.⁶⁶ While a state-by-state analysis of specific legislative objectives is not possible in a work of this length, states have reached different outcomes in crafting data notification statutes after balancing the interests at stake.⁶⁷ California's seminal statute blazed a trail for others to follow, but states have decided on important substantive variations.

Breach notification laws let individuals know that their data has slipped into unauthorized hands. As described in Part I.A, these variations are products of the different definitions states set for covered information as well as risk-based exemptions built into some state statutes. These technical differences mask the subtler reason for the divergence among state statutes: data protection principles are the

64. Ballon, *supra* note 40, at 149. For example, Indiana requires disclosure "without unreasonable delay," IND. CODE ANN. § 24-4.9-3-3 (LexisNexis 2006), and Minnesota and California each require notice in "the most expedient time possible and without unreasonable delay," CAL. CIV. CODE § 1798.29 (West 2009); MINN. STAT. ANN. § 325E.61 (West Supp. 2008).

65. TEX. BUS. & COM. CODE ANN. § 521.053(d) (Vernon Supp. 2009); *e.g.*, R.I. GEN. LAWS § 11-49.2-4 (Supp. 2008).

66. See CHRISTOPHER J. BOSSO ET AL., AMERICAN GOVERNMENT: CONFLICT, COMPROMISE, AND CITIZENSHIP 88-95 (2000) (providing background on the divergence of state law according to states' values).

State law . . . has a great deal to say about how long and where we go to school, at what age we can legally drive an automobile, how we get married (and maybe divorced), how we raise our children, the kinds of taxes we pay, when and where we buy liquor, the rules under which we run our businesses, the public services we receive, and how and where we are buried.

Id. at 93. For a discussion on the broader application of this point in Western civilization, see GUTWIRTH, *supra* note 2, at 88 (highlighting the relevance of "the origin, motivation, and goals" of data protection laws in a global context). "Because privacy is intimately interwoven with individual freedom, it is undefined, contextual, relational, and nonabsolute." *Id.* at 83.

67. See BOSSO ET AL., *supra* note 66, at 88-95. The National Conference of State Legislatures maintains a catalogue of state security breach disclosure laws. National Conference of State Legislatures, *supra* note 5. It also lists disclosure laws by year. National Conference of State Legislatures, Breach of Information, <http://www.ncsl.org/programs/lis/cip/priv/breach.htm> (last visited Nov. 9, 2009).

product of widely divergent and varied norms.⁶⁸ The main divergence in these norms is the distinction between “data security” and “information privacy.”⁶⁹

In thinking about data security, especially with respect to financial personally identifiable information, “[t]here is a tight link between failure to protect sensitive personal data and financial liability.”⁷⁰ In other words, the loss of control over a particular type of data—that which can be used to create false accounts or make unauthorized purchases—leads to measurable economic harm.⁷¹ Conversely, the concept of information privacy deals with harm that is more dignitary in nature: it is the unauthorized access to personal information that is troubling, though this may be difficult to measure in concrete terms.⁷² In this way, “‘privacy’ and ‘data control’ address vastly different public policy questions,”⁷³ especially from a consumer-protection perspective. Viewing the discourse surrounding data breach notification laws with these two different frames in mind, it is apparent that states have defined their laws to comport with either one or both of these interests.⁷⁴ Further complicating the balancing act is that states must also account for the effect notification laws have on businesses, with the resulting statute being more or less consumer friendly depending on how these balances have been struck.

1. Data Control: Financial Interests

One primary goal of notification statutes is to regulate data control in a way that minimizes the risk of pecuniary harm to consumers.⁷⁵ Much of data breach law has been enacted to deal with the threat of identity theft resulting from unauthorized access of computerized records, as opposed to a more-encompassing threat of

68. GUTWIRTH, *supra* note 2, at 88 (discussing data protection laws as growing out of different values based on the jurisdiction in which they are developed).

69. Janger & Schwartz, *supra* note 18, at 231.

70. *Id.* at 231–32 (noting that the overriding concern with entities that retain financial data is that unauthorized access leads to identity theft, not that the breaching entity will sell it to third parties as occurs with marketing data).

71. *Id.*

72. *Id.* at 231.

73. Raymond T. Nimmer, *Contracts, Markets, and Data Control*, in *SECURING PRIVACY IN THE INTERNET AGE*, *supra* note 15, at 325, 325.

74. For a full discussion, see *infra* Part II.

75. See, e.g., Kennedy & Kennedy, *supra* note 5, at 19 (“The premise of all of these laws is that prompt consumer awareness of unauthorized access to sensitive personal information is a key step in combating fraud and identity theft and in mitigating the consequences of both.”).

invasion of privacy.⁷⁶ But the theory of identity theft is a narrow one. The Federal Trade Commission defines identity theft as the use of an individual's personally identifiable information, including name, bank account information, or social security number, to commit fraud or another crime.⁷⁷ Understood this way, identity theft is the real interest at the heart of the notification laws, and yet "a lot of identity theft has nothing to do with data breaches."⁷⁸ Less than a quarter of people who have suffered identity theft-related losses point to a data breach as the reason.⁷⁹ Consequently, focusing on data security breaches is perhaps not the most effective way to address identity theft. Assuming, however, that breach notification laws provide some protection from economic harm, states must determine to what extent to provide additional protection to consumers at the expense of imposing additional costs on businesses.⁸⁰ In this calculus, states must decide whether to place the cost (a) entirely on consumers, as in states without breach notification laws, (b) entirely on businesses, as in states that provide for affirmative data protection regulations and for a private right of action for injured individuals to recover damages, or (c) somewhere in between.

The economic costs associated with data control violations can be stark for both consumers and businesses. The typical individual affected by a data breach in 2006 spent about four hours resolving identity theft issues (e.g., notifying credit reporting agencies and other authorities), with thirty percent of individuals spending less than an hour.⁸¹ The median value identity thieves obtained in that year amounted to \$500.⁸² Individuals might also incur miscellaneous expenses, such as postage and other fees, but fifty-nine percent of victims incurred no out-of-pocket expenses at all.⁸³ The out-of-pocket

76. See *infra* Part III.B.

77. Federal Trade Commission, Fighting Back Against Identity Theft: About Identity Theft, <http://www.ftc.gov/bcp/edu/microsites/idtheft/consumers/about-identity-theft.html> (last visited Nov. 18, 2009).

78. Fisher, *supra* note 24 (quoting Sasha Romanosky, a researcher at Carnegie Mellon University who studied Federal Trade Commission data on state breach notification laws).

79. *Id.*

80. See *supra* note 17 and accompanying text.

81. FED. TRADE COMM'N, 2006 IDENTITY THEFT SURVEY REPORT 39–40 (2007), available at <http://www.ftc.gov/os/2007/11/SynovateFinalReportIDTheft2006.pdf>. Sixty percent of victims whose identities were used to establish new accounts (as opposed to charges being incurred against existing accounts) spent more than ten hours resolving the issue. *Id.* at 40.

82. *Id.* at 6; Choi, *supra* note 7 (reporting that the average cost per incident in 2008 was \$496).

83. FED. TRADE COMM'N, *supra* note 81, at 37.

expenses typically incurred are small enough that *Consumer Reports* counsels that identity theft insurance is not even worth paying for.⁸⁴ In certain cases, however, victims might spend years trying to repair the damage to their records and might sustain losses of thousands of dollars.⁸⁵

Exerting pressure in the opposite direction of consumers' economic interests are the economic interests of the businesses maintaining the data. Unlike costs to consumers,⁸⁶ costs to businesses seem to be rising: one benchmark study estimates that the per-record cost to businesses of a data breach in 2007 was \$197, up from \$138 in 2005.⁸⁷ A 2008 estimate puts the average cost per record at \$202, or \$6.6 million per organization experiencing a breach.⁸⁸ More than half of this cost stems from lost business in the wake of a breach notification.⁸⁹ After disclosing a large breach in January 2009, Heartland Payment Systems stock decreased in value by forty-two percent.⁹⁰ Depending on how state laws are drafted and whether an obligation to notify is actually triggered, businesses may be exposed to these costs to a greater or lesser degree.

While it is difficult to compare the economic cost of a breach to a consumer directly to the cost to a business, the variation in the extent to which states have shifted the cost to one party or the other suggests that it is not just economic harm from which states wish to protect their citizens. The objectively low cost to the ordinary consumer is made possible by the costs businesses undertake in providing notice of a breach. But not only do businesses incur notice costs, they also suffer the attendant costs of lost business and stock devaluation in the wake of a breach.⁹¹ Some incur even further costs where states impose affirmative data protection measures.⁹² In some states, not only are

84. *Costly Credit-Monitoring Services Offer Limited Fraud Protection*, CONSUMERREPORTS.ORG, Apr. 2007, <http://www.consumerreports.org> (search "Costly credit-monitoring services"; then follow "Costly credit-monitoring services offer limited fraud protection 4/07" hyperlink).

85. Solove, *supra* note 25, at 114 (describing a worst-case scenario for an identity theft victim).

86. See *supra* note 7 and accompanying text.

87. PONEMON INST., *supra* note 7, at 8.

88. Brian Krebs, *Data Breaches Are More Costly Than Ever*, WASH. POST, Feb. 3, 2009, at D3 (including in this figure costs associated with hiring forensic experts, notifying customers, establishing free hotlines, and offering services to retain customers).

89. PONEMON INST., *supra* note 7, at 12.

90. Krebs, *supra* note 88.

91. See *supra* notes 89–90 and accompanying text.

92. See, e.g., Robert Mullins, *Understanding the Impact of New State Data Protection Laws*, SEARCHFINANCIALSECURITY.COM, Feb. 26, 2009, <http://searchfinancialsecurity.com>.

the risks skewed toward the corporation, but consumers are empowered with a private right of action in the event corporations do not follow notification laws.⁹³ States without a materiality requirement⁹⁴ impose these costs regardless of the risk of an individual's data actually being misused. The difference among these policy decisions lies in states' interpretation and protection of noneconomic factors underlying data protection laws.

2. Information Privacy: Dignitary Interests

Apart from the specific criminalization of all intrusions into personally identifiable information, the theory of identity theft is inadequate to address many data breach scenarios from a consumer-protection perspective.⁹⁵ An individual's commercial interest in avoiding exploitation of his personally identifiable information described above should be seen as distinct from a broader privacy right.⁹⁶ Many data breach cases that rest on the claim of increased susceptibility to identity theft fail where a plaintiff has not suffered compensable damages.⁹⁷ But beyond the financial interest in avoiding identity theft or fraud, there are other dignitary interests that some states choose to protect. Misappropriation or leakage of medical records may reveal information that would be embarrassing to the affected individual but not actually cause measurable damages.⁹⁸ Other states recognize a right of privacy based on some already-

techtargget.com/tip/0,289483,sid185_gci1349287,00.html (noting that states such as Massachusetts and Nevada are increasingly regulating data protection measures above and beyond notification, including requiring encryption and third-party compliance audits).

93. These states are in the minority and include California, Hawaii, Illinois, Louisiana, Maryland, New Hampshire, North Carolina, Tennessee, and Washington. CAL. CIV. CODE § 1785.15(f) (West 2009); HAW. REV. STAT. ANN. § 487N-3(b) (LexisNexis Supp. 2007); 815 ILL. COMP. STAT. ANN. 505/10a (West 2008); LA. REV. STAT. ANN. § 51:3075 (Supp. 2009); MD. CODE ANN., COM. LAW § 13-407 (LexisNexis 2005); N.H. REV. STAT. ANN. § 359-C:21(I) (LexisNexis 2008); N.C. GEN. STAT. § 75-65(i) (2007); TENN. CODE ANN. § 47-18-2104 (2001); WASH. REV. CODE ANN. § 19.255.010(10) (West 2007).

94. See *supra* Part I.A.2.

95. See *supra* notes 81–85 and accompanying text.

96. ROSEMARY JAY, DATA PROTECTION LAW AND PRACTICE 55 (3d ed. 2007).

97. Silverman, *supra* note 53, at 9 (discussing cases from Minnesota, Michigan, and Arizona in which the “mere threat of future harm” from identity theft was “insufficient” to state a claim).

98. See, e.g., *Randi A.J. v. Long Island Surgi-Center*, 842 N.Y.S.2d 558, 567 (N.Y. App. Div. 2007) (holding that a medical provider's wrongful disclosure to patient's mother of information implying patient obtained an abortion supported an award of punitive damages based on the center's “reckless disregard of the plaintiff's rights and expressed wishes”).

existing right, like property.⁹⁹ This conceptualization of personally identifiable information equates such data to property, over which the owner should have control to exclude others from viewing.¹⁰⁰ But instead of conceptualizing the action as one lying in trespass, the tort of invasion of privacy can be seen as an interest in itself, focusing instead on the right of a private person to be free from the “public gaze.”¹⁰¹ This understanding of privacy in connection with an individual’s personally identifiable information encompasses a range of reasons that the individual would wish for such data to remain private, none of which implicates financial harm.¹⁰² Beyond the tangible economic loss an individual might experience from unauthorized use of her personal data, she also experiences a nonpecuniary loss simply by virtue of losing control over that data.¹⁰³

Another construct of personally identifiable information is personal data as an item tradable for value: “To the extent that others value access to us, and use it to our benefit, our identity is an asset.”¹⁰⁴

99. 62A AM. JUR. 2D *Privacy* § 2 (2005) (citing *Schuyler v. Curtis*, 42 N.E. 22 (N.Y. 1895)).

100. *See, e.g.*, *Kaiser Aetna v. United States*, 444 U.S. 164, 176 (1979) (“[O]ne of the most essential sticks in the bundle of rights that are commonly characterized as property [is] the right to exclude others.”); JOSEPH WILLIAM SINGER, *ENTITLEMENT* 10 (2000) (discussing an understanding of property as including “[t]he right to exclude nonowners” and comprising “relations among persons with respect to the control and use of valued resources”).

101. 62A AM. JUR. 2D *Privacy* § 1 (citing *Allstate Ins. Co. v. Ginsberg*, 863 So. 2d 156, 162 (Fla. 2003)). This cause of action is to be distinguished from a constitutional right of privacy, which protects personal privacy against unlawful government invasion. *See, e.g.*, *United States v. Calandra*, 414 U.S. 338, 354 (1973) (“The purpose of the Fourth Amendment is to prevent unreasonable governmental intrusions into the privacy of one’s person, house, papers, or effects. The wrong condemned is the unjustified governmental invasion of these areas of an individual’s life.”). This theme would be fertile ground for additional research to the extent that the government is the entity responsible for collecting and securing personally identifiable information that is the subject of a breach, but will not be taken up in this Comment. For more background on the violation of privacy as a tort, see Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 195 (1890) (defining the right to privacy as “the right to be let alone”) and William L. Prosser, *Privacy*, 48 CAL. L. REV. 383, 389 (1960) (describing the tort of invasion of privacy).

102. *See Rode*, *supra* note 19, at 1608 (“[D]ata control is as much about traditional notions of privacy as it is about the relationships between individuals and businesses that process personal identification data.”).

103. Susan W. Brenner, *Cybercrime Metrics: Old Wine, New Bottles?*, 9 VA. J.L. & TECH. 13, 33–34 (2004) (discussing cyber crimes as resulting in a victim’s loss of control over her property).

104. John Deighton, *Market Solutions to Privacy Problems?*, in *DIGITAL ANONYMITY AND THE LAW* 137, 137 (C. Nicoll, J.E.J. Prins & M.J.M. van Dellen eds., 2003); *see also* GUTWIRTH, *supra* note 2, at 88 (“The motive driving the whole debate is the free flow of information, not privacy.”).

A simple example is found in the behavioral marketing data collected by supermarket loyalty cards. A “deal” is consummated in obtaining one: the consumer’s consent (often implied) to be a source of behavioral marketing data in exchange for discounts at the store.¹⁰⁵ Moreover, the “deal” often permits the supermarket to sell information it collects to third parties, further underscoring the nature of the information provided as an asset.¹⁰⁶ “Under a regulatory regime, [like the E.U.], . . . reselling of information is prohibited and the economic value of the information is lost. Under a market regime, the value is available to the manufacturers, improving the efficiency of marketing methods, but, more important, some of the value is captured by shoppers.”¹⁰⁷ Foregoing this membership may provide a measure of information privacy, but it comes at the cost of economic benefits.¹⁰⁸

Because customers do not provide billing information or social security numbers, misappropriated data of this type do not trigger state notification laws that are concerned with purely financial harm. But there is something unsettling about the idea of the whole world discovering the brand of condoms we select or the frequency with which we purchase wine or beer.¹⁰⁹ “Even likes, dislikes, habits, opinions and preferences are ‘indicia’ of identity insofar as they are capable of being used to track down a particular person.”¹¹⁰ While a breach involving these types of data may not result in financial harm to the consumer, he does not likely expect that collected and aggregated personal information will become available beyond the initial collection point.

105. See Lassow & Ourada, *supra* note 1, at 54.

106. See Deighton, *supra* note 104, at 140 (discussing how shoppers “sell” information about their purchases to stores for discounts).

107. *Id.* at 144. But see Lassow & Ourada, *supra* note 1, at 54 (questioning the degree to which consumers really benefit from shopper rewards programs).

108. See Deighton, *supra* note 104, at 140.

109. Indeed, attorneys are beginning to use records of grocery store purchases to impeach a client’s spouse in child-custody cases by noting regular purchases of tobacco and alcohol. See Joseph A. Bellizzi & Terry Bristol, *An Assessment of Supermarket Loyalty Cards in One Major US Market*, 21 J. CONSUMER MARKETING 144, 145 (2004) (citing a case in which the Drug Enforcement Administration subpoenaed a suspect’s loyalty card purchase history hoping to find “high-volume purchases of plastic sandwich bags” to prove the parent’s involvement in drug dealing).

110. Chris Nicoll, *Concealing and Revealing Identity on the Internet*, in DIGITAL ANONYMITY AND THE LAW, *supra* note 104, at 99, 99 (“[These types of data] are all part of a person’s profile and have a value to the subject’s tracker—often, as in the case of a direct marketer, they have a value that can be translated directly into cash.”).

C. Reconciling the Interests

With these different conceptualizations of privacy in mind, the source of the legal obligation and the obligation to individuals may vary depending on several aspects of the breach.¹¹¹ The nature of the data involved (i.e., whether it is a social security number, consumer marketing details, or health information) may determine whether there is a chance that the affected individual is likely to suffer economic or some other type of harm.¹¹² The nature of a company's business may dictate which, if any, regulators have jurisdiction over a breach.¹¹³ Contracts the company has with third parties may imply additional or different obligations if the company maintains data on behalf of those third parties.¹¹⁴ And, as mentioned above, the state(s) or nation(s) with which a company does business entails a variety of obligations because, by their terms, the various statutes address differing concerns.¹¹⁵

In setting data security policy, a state is pulled in at least four directions along two continuums. As described in Part I.B above, the first continuum pits data control against information privacy; that is, protecting only financial data or recognizing a wider dignitary interest in an individual's data. The second continuum pits consumer protection against business interests. Part II examines how states have reconciled these two continuums in their data breach notification laws.

II. STATE-BASED APPROACHES

Forty-five states plus Washington, D.C., Puerto Rico, and the U.S. Virgin Islands have enacted breach notification laws.¹¹⁶ State

111. Laudise, *supra* note 36, at 401; *see also* GUTWIRTH, *supra* note 2, at 86 (“[G]eneralizations are incompatible with the nature of privacy’s freedom. Privacy depends on context and on the specific relations between the different factors in each case—the respective interests of the people involved, their social role and impact on power, the aim of the disputed data processing, [and] the application of the data concerned.”).

112. Laudise, *supra* note 36, at 401.

113. *Id.* *See infra* Part II.B (discussing federal provisions covering certain types of data elements).

114. Laudise, *supra* note 36, at 401; *see also* *Sovereign Bank v. BJ’s Wholesale Club, Inc.*, 533 F.3d 162, 166 (3d Cir. 2008) (describing liability that arose out of a merchant agreement between Sovereign Bank and BJ’s Wholesale Club regarding failure to delete information stored on customers’ Visa cards).

115. *See* Laudise, *supra* note 36, at 401.

116. National Conference of State Legislatures, *supra* note 5. Only Alabama, Kentucky, Mississippi, New Mexico, and South Dakota had not enacted breach laws as of October 2009. *Id.*

breach notification laws exemplify the freedom states have traditionally had in defining corporate law and assigning values to the stakeholders in the marketplace.¹¹⁷ The American view of privacy rights has been influenced by individual self-determinism, which permits individual behavior to the extent that it does not harm others.¹¹⁸ “Americans have tended to reject overarching regulation in favour of a self-regulatory . . . approach.”¹¹⁹ Absent a federal law to deal with all data protection problems, states have taken a variety of measures to protect businesses and consumers, with each responding to the consumer–business and data protection–privacy dilemmas in different proportions.

A. State Laws Are Tailored to Protect Specific Interests

While states’ subsequent variations on California’s landmark statute have not been wildly innovative,¹²⁰ subtle differences in statutory scope and purpose have separated breach notification laws into those that protect only against economic harm and those that protect a broader information privacy interest in addition to pecuniary harm. Given that the broader the net of interests cast, the more notification will be required, states have struck different consumer–business and data protection–privacy balances.¹²¹ Part II.A reviews some of these choices.

A look at New Jersey’s breach notification statute is instructive in applying these two continuums of data security policy as an analytical framework.¹²² While New Jersey’s notification statute is planted firmly in the economic data control strand of the dichotomy based on its definition of personal information,¹²³ its state constitution has been construed to confer a privacy interest in an individual’s

117. See, e.g., Richard Briffault, *Federalism*, in THE OXFORD COMPANION TO AMERICAN LAW 299, 299 (Kermit L. Hall ed., 2002) (“We have not just one system of laws but fifty-one, with the states adopting their own rules in areas that comprise the core of civil society—contract, tort, property, criminal law, domestic relations, corporate law, and the regulation of the professions.”).

118. JAY, *supra* note 96, at 3 (comparing the U.S. and European approaches to data protection law and contrasting the systems’ philosophical underpinnings).

119. *Id.*

120. See Brandon Faulkner, Comment, *Hacking into Data Breach Notification Laws*, 59 FLA. L. REV. 1097, 1105 (2007).

121. Deighton, *supra* note 104, at 139 (noting that subtle variations in privacy policy choices can lead to great variation in security policy objectives).

122. See *supra* Part I.C.

123. See N.J. STAT. ANN. § 56:8-161 (West 2008) (restricting personal information to data elements whose misuse would result in financial harm).

social security number.¹²⁴ The New Jersey Superior Court Appellate Division has held that this privacy interest outweighs even a record collector's interest in obtaining the data under the state's open records laws.¹²⁵ Therefore, while the New Jersey statute arguably protects chiefly financial interests, the New Jersey courts are likely to hold that the statute also protects some notion of a dignitary interest in one's information. On the consumer-business continuum, the statute's purpose appears to be virtually all-encompassing, requiring businesses to disclose "any breach of security of those computerized records following discovery or notification of the breach to any customer who is a resident of New Jersey whose personal information was, or is reasonably believed to have been, accessed by an unauthorized person."¹²⁶ This seemingly sweeping consumer protection is tempered, however, by a provision permitting businesses to develop and implement their own security policy for notification procedures: provided that the notification requirements are consistent with the New Jersey data breach statute, businesses retain discretion to determine when unauthorized access has occurred.¹²⁷ The statute thus provides broad consumer protection, balanced against businesses' judgment to carry out the disclosure.

In some states, such as Iowa and Rhode Island, the interest protected by notification laws is strictly financial: notice is not required where "no reasonable likelihood of financial harm to the consumers whose personal information has been acquired has resulted or will result from the breach."¹²⁸ Unlike the New Jersey statute, however, businesses in Iowa and Rhode Island can determine that notification is not required only by working in conjunction with

124. *Social Security Numbers: New Jersey Recognizes Privacy Interest in Social Security Numbers in State Records*, Privacy Law Watch (BNA) (Sept. 12, 2008) (only available through online subscription service) (noting the state supreme court has found "a constitutional right of privacy, including the disclosure of confidential or personal information" (quoting *Burnett v. County of Bergen*, 954 A.2d 483, 491 (N.J. Super. Ct. App. Div. 2008))).

125. *See Burnett v. County of Bergen*, 954 A.2d 483, 495 (N.J. Super. Ct. App. Div. 2008) ("Under these circumstances, the SSN becomes a key to access a myriad of information about an individual, such as government filings containing a person's physical description, race, nationality, gender, family life, marital relationship, residence, location, contact information, political activity, financial condition, employment, criminal history, health and medical condition, and other personal information.").

126. § 56:8-163(a) (emphasis added).

127. § 56:8-163(e).

128. IOWA CODE ANN. § 715C.2(6) (West Supp. 2009); R.I. GEN. LAWS § 11-49.2-3(a) (Supp. 2008) (requiring disclosure of security breach that "poses a significant risk of identity theft").

law enforcement.¹²⁹ Oregon's Consumer Identity Theft Protection Act¹³⁰ is also tailored to protect economic interests and similarly requires cooperation with law enforcement to make a determination on whether disclosure is required.¹³¹

Missouri, the most recent state to enact a breach notification law,¹³² had previously considered a bill that covered the data elements typical to the protection of economic interests.¹³³ While the reason for the initial and long-prevailing resistance to the bill is unclear, there is some evidence that the state's valuation of consumer interests versus business interests simply came out the opposite way from Iowa's, Rhode Island's, and Oregon's.¹³⁴ In the end, however, Missouri enacted a breach law that encompasses health and medical information,¹³⁵ suggesting not only that consumers won out over businesses but also that dignitary interests prevailed over purely financial ones.

Recognizing a broader information privacy interest protected by notification laws, Montana enacted its breach law to "enhance the protection of individual privacy and to impede identity theft,"¹³⁶ language that suggests the broader privacy right is at least as important as protection from financial harm. California's definition of personally identifiable information includes medical records and health information,¹³⁷ Arkansas's Personal Information Protection

129. IOWA CODE ANN. § 715.C.2 (West Supp. 2009); R.I. GEN. LAWS § 11-49.2-4 (Supp. 2008).

130. OR. REV. STAT. § 646A.600 (2007).

131. OR. REV. STAT. § 646A.604(3) (2007).

132. MO. REV. STAT. § 407.1500 (West, Westlaw through 2009 First Regular Sess.).

133. S.B. 680, 93d Gen. Assem., 2d Sess. (Mo. 2006) The bill defined personal information to include, along with an individual's name, "(a) Social security number; (b) Driver's license number; (c) account number, credit card number, or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account." *Id.* The statute ultimately took effect on August 28, 2009, and unlike the bill previously debated, it covers medical and health information.

134. *See, e.g.*, Missouri Attorney General Web site, Consumer Blog: Data Breach Notification Laws, http://ago.mo.gov/ConsumerCorner/blog/10416/Data_breach_notification_laws/ (June 3, 2008, 10:38 CST) (alerting consumers that if a company doing business in Missouri loses consumers' personal information, it is under no obligation to disclose the breach). A breach law has since been enacted in Missouri. *See* MO. REV. STAT. § 407.1500 (2009).

135. MO. REV. STAT. § 407.1500 (West, Westlaw through 2009 First Regular Sess.) (defining health insurance information and medical information and including the terms within personal information).

136. MONT. CODE ANN. § 30-14-1701 (2009).

137. CAL. CIV. CODE § 1798.29 (West 2009).

Act¹³⁸ also protects medical information.¹³⁹ Nebraska's definition includes "unique biometric data, such as a fingerprint, voice print, or retina or iris image, or other unique physical representation."¹⁴⁰ While most of these data components are the type that one day may be used routinely to access financial accounts, and are thus poised to protect economic data, the term "other unique physical representation" has yet to be construed by a court. Interpreting the term broadly, it would not be absurd to argue that in Nebraska, the unauthorized access of an individual's first and last name plus an image of that individual would trigger an obligation to notify. Wisconsin also includes the "other unique physical representation" language and adds to it a person's DNA profile.¹⁴¹

California has included within its notification statute a provision speaking directly to information privacy violations that arise when a business discloses a wide range of noneconomic data to a third party as part of a direct marketing scheme.¹⁴² The triggering categories include: name, address, telephone number, or e-mail address; age or date of birth; number, names, addresses, ages, gender, or e-mail addresses of individual's children; individual's height, weight, race, religion, occupation, education, or political party affiliation; and medical condition.¹⁴³ This statute, and others like it, represent the wide range of information protected by breach notification laws in various jurisdictions.

Just as state law has proven flexible enough to embrace different combinations of the data control–privacy and consumer–business continuums, a state-based approach also permits states to include data protection measures. Some states have begun to layer affirmative data protection obligations over notification laws, requiring businesses in their jurisdictions to provide security measures for personally identifiable information.¹⁴⁴ These regulations generally obligate companies to protect particular categories of personal data

138. 2005 Ark. Acts 4867 (codified at ARK. CODE ANN. § 4-110 (Supp. 2009)).

139. ARK. CODE ANN. § 4-110-103(5) (Supp. 2009) (" 'Medical information' means any individually identifiable information, in electronic or physical form, regarding the individual's medical history or medical treatment or diagnosis by a health care professional.").

140. NEB. REV. STAT. § 87-802(5)(e) (2008).

141. WIS. STAT. ANN. § 134.98 (West 2008).

142. CAL. CIV. CODE § 1798.83(a) (West 2009).

143. *Id.* § 1798.83(e). Violations of this provision can result in a civil penalty up to \$3,000, civil damages, or injunctive relief. *Id.* § 1798.84.

144. Smedinghoff, *supra* note 1, at 26. These states include Arkansas, California, Maryland, Massachusetts, Nevada, Oregon, Rhode Island, Texas, and Utah. *Id.* at 26 & n.23.

such as social security numbers or credit card information.¹⁴⁵ In Minnesota, retailers that violate a forty-eight-hour restriction on the amount of time credit card transaction data may be stored are liable to financial institutions for the costs of canceling or reissuing cards.¹⁴⁶ A Nevada law that took effect in October 2008 requires businesses to encrypt personally identifiable customer details that are electronically transmitted but caps damages at \$1,000 per customer per occurrence.¹⁴⁷ Effective in January 2010, Massachusetts will require businesses that collect information about state residents to encrypt data stored on mobile devices.¹⁴⁸ States' current ability to layer proactive, protective measures over reactive, retributive measures further enhances legislatures' power to craft law to best suit states' needs.¹⁴⁹

Not only have some states tailored their breach laws to include affirmative consumer protection measures, but states have also designed data protection laws to dial up or down the threshold for standing, actionable claims, and liability. States (in part through their courts) define who has standing to bring suit, limiting or enlarging the pool of potential plaintiffs according to the criteria each state values. As noted in Part I.A above, a private right of action for violations of notification statutes exists in a minority of states.¹⁵⁰ Virginia's notification law does not expressly provide for individuals to file lawsuits to recover actual damages, but it does include language that preserves an individual's right to recover direct economic damages from a violation of the breach laws.¹⁵¹ In most other states, enforcement of breach notification laws is left to the state attorney general.¹⁵²

145. *Id.* at 58 (noting that if a company continues collecting data of a covered type, it must implement heightened security measures for that data).

146. Thomas, *supra* note 3, at 369; Graves, *supra* note 23, at 1132.

147. Worthen, *supra* note 23.

148. Robert Westervelt, *Massachusetts Data Protection, Encryption Law Extended*, SEARCHSECURITY.COM, Feb. 13, 2009, http://searchsecurity.techtarget.com/news/article/0,289142,sid14_gci1347836,00.html#.

149. See Worthen, *supra* note 23. In Massachusetts, companies appear resigned to such heightened requirements: "It's a burden, . . . but it's something you have to do." *Id.* (quoting Karen Grant, a Massachusetts-based hospital operator). Estimated costs for complying with the heightened security requirement include a projected \$3,000 initial outlay and \$500 per month in maintenance. *Id.*

150. See *supra* note 93 and accompanying text.

151. Donald G. Alpin, *Breach Laws Taking Effect Soon in Three States Have Significant Differences*, Privacy Law Watch (BNA) (June 26, 2008) (only available through online subscription service).

152. Silverman, *supra* note 53, at 8.

Whether the suit is brought by an individual or by the attorney general, states also differ as to what rises to an actionable claim. In Ohio, the “mere increased risk of identity theft is not sufficient harm to create standing.”¹⁵³ But in California, a federal district court conferred preliminary standing where a plaintiff alleged his risk of identity theft had increased because of a data breach, without showing measurable damages.¹⁵⁴ Along with enforcement, differences among states abound with regard to the liabilities imposed on a company that disregards its obligation to notify under state law.¹⁵⁵ Provisions range from an administrative fine for each day a breach is not disclosed¹⁵⁶ to damages or injunctive relief under a civil action.¹⁵⁷

B. State Laws Are Already Supplemented by Federal, Industry-Specific Laws

Unlike state laws, which try to balance competing interests in a single statute, federal industry-specific laws take a risk-assessment approach geared specifically toward the type of data breach and the particular interest the agency or sector guidelines seek to protect.¹⁵⁸ For instance, the medical information protected by the Health Insurance Portability and Accountability Act (“HIPAA”)¹⁵⁹ is of a different character than financial data protected by the Gramm-Leach-Bliley Act (“GLBA”)¹⁶⁰ and the Fair and Accurate Credit Transaction Act (“FACTA”),¹⁶¹ with different consequences for individuals flowing out of a breach of either type. In this manner, security guidelines and, more important, notification procedures in

153. Thomas, *supra* note 3, at 370.

154. Ruiz v. Gap, Inc., 540 F. Supp. 2d 1121, 1126 (N.D. Cal. 2008) (“[T]he fact that Plaintiff faces an increased risk that his identity may be stolen at some time in the future—seems, at first blush, conjectural or hypothetical, rather than actual or imminent. Nonetheless, the Court . . . cannot conclude that Ruiz lacks standing.”).

155. Faulkner, *supra* note 120, at 1113.

156. *E.g.*, FLA. STAT. ANN. § 817.5681(2)(b) (West 2006).

157. *E.g.*, CAL. CIV. CODE § 1798.84 (West 2009); *see also* Faulkner, *supra* note 120, at 1113 (summarizing the spectrum of liability provisions in state data breach laws).

158. Picanso, *supra* note 23, at 362.

159. Health Insurance Portability and Accountability Act (HIPAA) of 1996, Pub. L. No. 104-191, 110 Stat. 1936 (codified as amended in scattered sections of 18, 26, 29, and 42 U.S.C.). The privacy regulations are codified at 45 C.F.R. pts. 160, 164 (2008 & Supp. 2009).

160. Gramm-Leach-Bliley Financial Modernization Act, Pub. L. No. 106-102, 113 Stat. 1338 (1999) (codified as amended in scattered sections of 12, 15, and 16 U.S.C.).

161. Fair and Accurate Credit Transactions Act (FACTA) of 2003, Pub. L. No. 108-159, 117 Stat. 1952 (codified as amended in scattered sections of 15 U.S.C.) (amending the Fair Credit Reporting Act of 1970, Pub. L. No. 91-508, 84 Stat. 1114 (codified as amended at 15 U.S.C. §§ 1681–1681x)).

the event of a breach, are tailored to the type of data and the type of risk rather than being based on blanket technical criteria.¹⁶² Indeed, the heart of these federal provisions is not notification but rather protection, underscoring the misleading nature of the federal breach law discourse: disclosure may not always be the best tool to guard all implicated interests. The GLBA, FACTA, and HIPAA are examples of industry standards that protect discrete, regulable data segments, giving individuals a baseline of protection in these areas while not foreclosing states from implementing more robust measures.

The GLBA was enacted in 1999¹⁶³ to establish security regulations for the financial services industry. The purpose of the GLBA is to facilitate financial information sharing among institutions and banks within a framework that protects clients' rights.¹⁶⁴ Federal institutions falling within the GLBA cannot disclose personal information without first notifying customers of the institution's disclosure policies and providing an opportunity to "opt-out."¹⁶⁵ To comply with the GLBA's disclosure requirements, financial institutions must develop data security policies, provide consumers with information regarding data disclosure (including the opportunity to opt-out of information-sharing with third parties), and notify customers when a breach leads to (or could reasonably lead to) the misuse of customer information.¹⁶⁶ An exception to the GLBA permits disclosure to comply with the judicial process, including discovery requests.¹⁶⁷

The GLBA only supersedes state or local laws to the extent that they are inconsistent.¹⁶⁸ The GLBA's savings clause provides that "a State statute, regulation, order, or interpretation is not inconsistent . . . if the protection such statute, regulation, order, or interpretation affords any person is greater than the protection provided under [the GLBA]."¹⁶⁹ This means that, within its mandate, the GLBA already

162. Picanso, *supra* note 23, at 376.

163. Gramm-Leach-Bliley Financial Modernization Act, Pub. L. No. 106-102, 113 Stat. 1338 (1999) (codified as amended in scattered sections of 12, 15, and 16 U.S.C.).

164. MARK OSBORNE, *HOW TO CHEAT AT MANAGING INFORMATION SECURITY* 84 (2006).

165. Richard J. Link, Annotation, *Validity, Construction, and Application of Information Privacy Provisions of Gramm-Leach-Bliley Act*, 5 A.L.R. FED. 2d 497, 497 (2005).

166. Picanso, *supra* note 23, at 367.

167. See *Martino v. Barnett*, 595 S.E.2d 65, 72 (W. Va. 2004).

168. See Link, *supra* note 165, at 507.

169. 15 U.S.C. § 6807(b) (2006). *But see* Anne P. Fortney, *Uniform National Standards for a Nationwide Industry: FCRA Preemption of State Laws Under the FACT Act*, 58

functions as a baseline for breach notification with regard to financial data, allowing state statutes to function as a one-way ratchet to increase notification obligations if desired. The GLBA does not create a private right of action.¹⁷⁰

Along with the GLBA, FACTA aims to protect consumers against identity theft by implementing technical standards for various data elements.¹⁷¹ For example, FACTA requires anyone accepting credit or debit cards for business transactions to truncate account numbers to no more than five digits on statements or receipts and prohibits printing the card's expiration date.¹⁷² From a consumer standpoint, however, FACTA can be seen as a concession in that "consumers came out on the losing end when Congress virtually barred states from adopting stronger laws,"¹⁷³ particularly as compared to states empowering individuals with a private right of action. Privacy activists believe that "FACTA does little to make our personal information more secure" in the long run because it "preempts more protective state laws."¹⁷⁴ In other words, FACTA is useful in providing a baseline protection for discrete data elements like credit card numbers, but does not effectively address wider privacy interests.¹⁷⁵

Recognizing that an individual has a privacy interest in her medical information, HIPAA deals with personal health data, which is defined as

CONSUMER FIN. L.Q. REP. 259, 261 (2004) (noting that the GLBA may not prevent preemption of state or industry notice requirements by other statutes).

170. *Borinski v. Williamson*, No. Civ.A. 3:02-CV-1014, 2004 WL 433746, at *3 (N.D. Tex. Mar. 1, 2004) ("[The GLBA] shall be enforced by the Federal functional regulators, the State insurance authorities, and the Federal Trade Commission with respect to the [sic] financial institutions and other persons subject to their jurisdiction." (quoting 15 U.S.C. § 6805 (2006)). *But see* *Dunmire v. Morgan Stanley DW, Inc.*, No. 14-1059-CV-W-ODS, 2005 WL 1005993, at *2 (W.D. Mo. Apr. 7, 2005) (finding that financial institution's alleged violations of GLBA were enough to defeat a motion to dismiss for failure to state a claim).

171. Fair and Accurate Credit Transactions Act (FACTA) of 2003, Pub. L. No. 108-159, 117 Stat. 1952 (codified as amended in scattered sections of 15 U.S.C.) (amending the Fair Credit Reporting Act of 1970, Pub. L. No. 91-508, 84 Stat. 1114 (codified as amended at 15 U.S.C. §§ 1681-1681x)); Solove, *supra* note 25, at 116-17 (addressing how FACTA deals with misuse of data); Privacy Rights Clearinghouse, FACTA, The Fair and Accurate Credit Transactions Act: Consumers Win Some, Lose Some, <http://www.privacyrights.org/fs/fs6a-facta.htm> (last visited Nov. 18, 2009) (summarizing FACTA provisions from a consumer-protection perspective).

172. 15 U.S.C. § 1681c (2006) (amending the Fair Credit Reporting Act of 1970, 15 U.S.C. § 1681c(g)(1) (2000)).

173. Privacy Rights Clearinghouse, *supra* note 171.

174. Solove, *supra* note 25, at 117.

175. *See* Privacy Rights Clearinghouse, *supra* note 171.

information that is a subset of health information, including demographic information collected from an individual, and:

(1) Is created or received by a health care provider, health plan, employer, or health care clearinghouse; and

(2) Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and

(i) That identifies the individual; or

(ii) With respect to which there is a reasonable basis to believe the information can be used to identify the individual.¹⁷⁶

The Act's purpose is to protect the confidentiality, integrity, and availability of the data that health care providers manage (i.e., store, maintain, or transmit).¹⁷⁷ HIPAA is intended to "strike[] a balance that permits important uses of information, while protecting the privacy of people who seek care and healing. Given that the health care marketplace is diverse, [HIPAA] is designed to be flexible and comprehensive to cover the variety of uses and disclosures that need to be addressed."¹⁷⁸ HIPAA requires health care providers to notify patients of the organization's privacy policies and procedures and to obtain consent and authorization-of-use forms, but it originally did *not* require entities to notify individuals after unauthorized disclosure of health information.¹⁷⁹ HIPAA also permits broad exceptions in health care providers' privacy policies to allow disclosure pertaining to the protection of public health, essential government functions, law enforcement purposes, and as authorized by programs such as

176. 45 C.F.R. § 160.103 (2008). HIPAA uses the term "individually identifiable health information" to refer to personal health data. 42 U.S.C. § 1320d (2006).

177. § 160.164.

178. OFFICE FOR CIVIL RIGHTS, U.S. DEP'T OF HEALTH & HUMAN SERVS., SUMMARY OF THE HIPAA RULE: HIPAA COMPLIANCE ASSISTANCE 1 (2003), *available at* <http://www.hhs.gov/ocr/privacy/hipaa/understanding/summary/privacysummary.pdf>.

179. Faulkner, *supra* note 120, at 1116. Health and Human Services has since promulgated regulations implementing new breach notification requirements, obligating health care providers to issue written notice to individuals affected within thirty days of discovery of a breach. *See* Breach Notification for Unsecured Protected Health Information, 74 Fed. Reg. 42,740, 42,748–50 (Aug. 24, 2009) (to be codified at 45 C.F.R. pts. 160, 164). The new notification regulation went into effect on September 23, 2009. *See id.*

workers' compensation.¹⁸⁰ Failing to comply with HIPAA regulations can lead to civil and criminal penalties of up to \$1.5 million or ten years' imprisonment.¹⁸¹ Like the GLBA, HIPAA does not create a private right of action.¹⁸² Responsibility for enforcement of HIPAA rests with the Office for Civil Rights, a department within Health and Human Services that can take action on individual complaints and impose civil penalties.¹⁸³

The federal, industry-specific laws—including the GLBA, FACTA, and HIPAA—protect personally identifiable information where consensus exists that notification is a meaningful way to safeguard discrete interests. Recognizing that there probably is some core of sensitive information for which all individuals—regardless of their state of domicile—deserve protection, carefully circumscribed federal laws achieve this goal. The laws do so by precisely defining the type of data at issue and the circumstances under which disclosure is triggered and by tailoring the definition of personally identifiable information, the scope of the statute (and exceptions thereto), and the form of notice according to the relevant industry. In the medical information arena, even where a state does not recognize a privacy interest in health information, or where a state prefers not to enact a breach law at all, HIPAA offers individuals some baseline protection in the form of notice.¹⁸⁴ In this way, the industry-specific notification laws adequately supplement state notification laws. Part III reveals how a uniform, preemptive federal law would flatten the distinctions drawn among industries and across states.

III. THE FEDERAL PROPOSALS

Despite the dozens of federal data breach notification bills that have been introduced since the 109th Congress, none has garnered

180. OFFICE FOR CIVIL RIGHTS, *supra* note 178, at 6–9.

181. Act of Feb. 17, 2009, Pub. L. No. 111-5, § 13410(d)(1)–(3), 123 Stat. 271, 272–73; *see also* Am. Med. Ass'n, HIPAA Violations and Enforcement, <http://www.ama-assn.org/ama/home/index.shtml> (search “HIPAA Violations and Enforcement” using quotation marks; then follow hyperlink) (last visited Nov. 9, 2009) (summarizing HIPAA violations and enforcement provisions).

182. *Runkle v. Gonzales*, 391 F. Supp. 2d 210, 237 (D.D.C. 2005) (“Although HIPAA provides for civil and criminal penalties against those who improperly disclose an individual’s health information, ‘the law specifically indicates that the Secretary of HHS shall pursue the action against an alleged offender, not a private individual.’”) (quoting *Logan v. Dep’t of Veterans Affairs*, 357 F. Supp. 2d 149, 155 (D.D.C. 2004)).

183. *How is the HIPAA Privacy Rule Enforced?*, HIPAA MONTHLY, (HealthPort, Alpharetta, Ga.) Feb. 2008, at 1, 1, <http://www.healthport.com/viewDocument.aspx?id=282>.

184. *See* OFFICE FOR CIVIL RIGHTS., *supra* note 178, at 1, 17.

the requisite consensus to pass.¹⁸⁵ Still, calls for a uniform standard only seem to be increasing.¹⁸⁶ Before exposing the limitations of a uniform federal data breach notification law in Part IV, this Part reviews both the argument for a federal standard and the provisions that lawmakers have sought to include in a federal version of a breach law. These proposed laws fail to account for the different types of interests that state legislatures have considered¹⁸⁷ and hastily impose a one-size-fits-all solution, both obscuring the non-notification-based tools that might better protect data and privacy and hampering states' ability to impose tougher standards.¹⁸⁸

A. *Arguments for a Federal Standard*

Proponents of a single federal standard point to the reduced transaction costs of compliance as compared to the current multifarious regime.¹⁸⁹ The argument runs that currently too many regulations exist and that they are too confusing to comply with,¹⁹⁰ requiring companies to be aware of the requirements in each jurisdiction in which they do business and tailor each notice accordingly. Different thresholds for when notification is required, as well as different requirements as to the content of the notification, mean that companies doing business in several states must either comply with several sets of notification laws or apply the law of the state that has the most stringent requirements.¹⁹¹ Supporters of a federal regime criticize the state-based system, predicting that even if a company complies with the different standards across states, the existence of a varied response could expose the company to actions challenging the reasonableness of the initial risk assessment and

185. Data Security Breach Laws Remain the Province of the States, Future of Privacy Forum, <http://www.futureofprivacy.org/2009/01/06/data-security-breach-laws-remain-the-province-of-the-states/> (Jan. 6, 2009).

186. Declan McCullagh, *Can Congress Be Trusted to Secure Data?*, CNET NEWS, Apr. 3, 2006, http://news.cnet.com/Can-Congress-be-trusted-to-secure-data/2010-1029_3-6056763.html ("Everyone in Washington seems to think the feds need to step in and knit together a blanket of regulations that deal with a string of embarrassing security breaches.").

187. *See supra* Part II.

188. *See supra* note 23 and accompanying text (questioning the extent to which data breach notification laws ultimately benefit consumers).

189. *See, e.g.*, Jon Oltsik, *Why a National Data Breach Notification Law Makes Sense*, CNET NEWS, Apr. 14, 2009, http://news.cnet.com/8301-1009_3-10219135-83.html (including greater simplicity and reduced costs as reasons for supporting a federal standard).

190. Picanso, *supra* note 23, at 373.

191. Kennedy & Kennedy, *supra* note 5, at 28; Goodchild, *supra* note 16.

policy itself.¹⁹² Supporters, including many businesses, argue that a federal solution would likely reduce the time and cost of compliance for companies by providing a unified set of breach and compliance criteria.

B. A Survey of Key Bills Pending in Congress

Since California passed its trailblazing notification statute in 2003, members of Congress have submitted dozens of bills that would impose a national, uniform standard for breach notification laws. As illustrated below, the federal bills provide less protection to consumers than the state versions, even though it is in the name of consumer protection that the bills have been introduced.¹⁹³ The 111th Congress has continued the trend that began in 2005 of considering federal legislation for data security. Senator Dianne Feinstein reintroduced the Data Breach Notification Act (S. 139) in January 2009,¹⁹⁴ which would require federal agencies and businesses that store personally identifiable information to disclose a security breach to affected U.S. residents. The bill expressly preempts state laws relating to notification.¹⁹⁵ The scope of “personally identifiable information” is consistent with the data-control-oriented

192. Goodchild, *supra* note 16; *see also* Rode, *supra* note 19, at 1633 (“[E]xisting state notification statutes expose multistate corporations to increased liability. A uniform law offers the logical and practical next step.”). Proponents of the federal-law solution offer that the array of laws with which a company may need to comply increases that company’s exposure to liability for noncompliance. *See* Rode, *supra* note 19, at 1623 (citing 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, 31 (2003) (describing the difficulty in maintaining current resident status for data subjects and how this could cause a company to run afoul of the notification requirements)). A more extreme view contends that a company deploying varying notification standards by state is already operating on a negligent basis. *Id.* (citing Tyler Paetkay & Roxanne Torabian-Bashardoust, *California Deals with ID Theft: The Promise and the Problems*, BUS. L. TODAY, May–June 2004, at 37, 37 (highlighting the viability of a negligence suit by non-residents who did not receive notice about a breach against a company that only notified residents)).

193. *See, e.g.*, 155 Cong. Rec. S7871 (daily ed. July 22, 2009) (“The Personal Data Privacy and Security Act will help to meet this challenge, by better protecting Americans from the growing threats of data breaches and identity theft.”) (statement of Sen. Leahy).

194. CongressDaily, *Feinstein Introduces Data Security Bills*, NEXTGOV, Jan. 7, 2009, http://www.nextgov.com/nextgov/ng_20090107_1108.php; *see* Data Breach Notification Act, S. 139, 111th Cong. (2009); Notification of Risk to Personal Data Act, S. 239, 110th Cong. (2007) (110th Congress version).

195. S. 139, § 10 (“The provisions of this Act shall supersede any other provision of Federal law or any provision of law of any State relating to notification by a business entity engaged in interstate commerce or an agency of a security breach, except as provided in section 5(b).”). Section 5(b) merely permits a state to require that notice include victim-assistance information provided in that state. *Id.* § 5(b).

understanding of notification laws discussed in Part I.B above,¹⁹⁶ and the bill provides an exemption for breaches that do not pose a significant risk of harm as well as for breaches in which personally identifiable information was redacted or encrypted.¹⁹⁷ The bill does not cover health insurance or medical information and applies only to records in electronic or digital format.¹⁹⁸ The bill provides for enforcement by the Attorney General and state attorneys general, caps civil penalties against businesses, and does not grant a private right of action.¹⁹⁹ Other provisions include notifying the Secret Service when the number of individuals whose sensitive personally identifying information was breached exceeds 10,000 or when the data system that was breached contains more than one million individuals nationwide.²⁰⁰

Following the lead set by Senator Feinstein in her first round of bill proposals for the new Congress, measures similar to those introduced in the 110th Congress have been reintroduced.²⁰¹ Like S. 139, those measures are also closely tied to data control to the exclusion of information privacy; that is, notification is only triggered where there is some risk of measurable financial harm. For example, Representative Bobby Rush's bill, the Data Accountability and Trust Act (H.R. 2221), was reintroduced in the House on April 30, 2009,

196. See *supra* text accompanying notes 75–76. Senate Bill 139 uses the definition set out in 18 U.S.C. § 1028(d)(7):

any name or number that may be used, alone or in conjunction with any other information, to identify a specific individual, including any—(A) name, social security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number; (B) unique biometric data, such as fingerprint, voice print, retina or iris image, or other unique physical representation; (C) unique electronic identification number, address, or routing code; or (D) telecommunication identifying information or access device.

S. 139, § 13(5); 18 U.S.C. § 1028(d)(7) (2006).

197. S. 139, § 3(b).

198. See S. 139.

199. S. 139, §§ 8–9.

200. S. 139, § 7. Although the U.S. Secret Service has jurisdiction over financial fraud, it does not typically exercise this authority over individual cases unless they are connected to more widespread acts of criminal fraud or exceed a substantial dollar amount. Privacy Rights Clearinghouse, Identity Theft: What to Do if It Happens to You, <http://www.privacyrights.org/fs/fs17a.htm#11> (last visited Nov. 19, 2009). See generally Financial Crimes Division, U.S. Secret Serv., http://www.treas.gov/usss/financial_crimes.shtml (last visited Nov. 19, 2009) (outlining the duties of the U.S. Secret Service with respect to crimes concerning financial institutions).

201. E.g., H.R. Res. 31, 111th Cong. (2009) (kicking off the session by passing a bill “[e]xpressing support for designation of January 28, 2009, as ‘National Data Privacy Day’”).

and delegates authority to the Federal Trade Commission to promulgate regulations dealing with data security policies and procedures.²⁰² The bill sets the threshold for notification high relative to many states' standards: "Companies do not have to initiate such notices of [sic] they determine that 'there is no reasonable risk of identity theft, fraud or other unlawful acts.'"²⁰³ The Data Accountability and Trust Act leaves it to companies to decide whether and when to notify consumers, reducing the incentive for companies to independently develop security infrastructure and policies.²⁰⁴ Proposed H.R. 2221 also preempts state data security laws. A third data breach law introduced in the 111th Congress is Senator Patrick Leahy's Personal Data Privacy and Security Act (S. 1490).²⁰⁵ Like S. 139 and H.R. 2221, this bill preempts state breach laws.²⁰⁶ It also exempts business entities whose use of personally identifiable information is limited to fewer than 10,000 U.S. persons, as well as businesses that encrypt data.²⁰⁷

The proposals for a uniform data breach notification standard dramatically undercut many of the state-based provisions, reducing the scope of protected information and the cases in which notification would be triggered. In part because of jurisdictional disagreements over key terms, each federal proposal so far focuses on relatively uncontroversial financial harm and ignores individuals' dignitary interests.²⁰⁸

IV. WHY A FEDERAL LAW IS NOT THE SOLUTION

As outlined in Part III.B, the proposed federal bills largely tie notification requirements to identity theft, equating the interest that

202. Data Accountability and Trust Act, H.R. 2221, 111th Cong. (2009). The bill was introduced in substantially the same form in the previous two Congresses as H.R. 4127 (109th Cong.) and H.R. 958 (110th Cong.). See H.R. 958, 110th Cong. (2007); H.R. 4127, 109th Cong. (2005).

203. *Data Accountability and Trust Act: Hearing on H.R. 2221 Before the Subcomm. on Consumer Protection of the H. Comm. on Energy and Commerce*, 111th Cong. 5 (2009), available at http://energycommerce.house.gov/Press_111/20090505/transcript_20090505_ct.pdf (quoting Data Accountability and Trust Act, H.R. 2221, 111th Cong. (2009)).

204. *Id.*

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

206. *Id.* § 203 ("No requirement or prohibition may be imposed under the laws of any State with respect to any subject matter regulated under section 201, relating to individual access to, and correction of, personal electronic records held by data brokers.").

207. *Id.* §§ 301, 312.

208. See *supra* notes 202–06 and accompanying text.

the laws seek to protect with the risk of financial harm.²⁰⁹ The flaw in this approach is evident when compared to the different blends of interests the various state laws have addressed:²¹⁰ a federal law flattens the distinctions states have drawn along the data control–information privacy and the consumer protection–business interest continuums. Part IV.A explores the idea that, in a federal system, it is best to let states decide where to draw this balance, rather than imposing a single value judgment across the entire country. Part IV.B looks at the effect of federal preemption of state laws in jurisdictions that have opted for blends of values that are inconsistent with the federal proposals. Part IV.C argues that, in light of rapidly changing technology and concomitant security threats, a federal law would be too inflexible to safeguard even purely economic interests in anything but the shortest of terms. Variables such as the scope of protection, the definition of information covered, inclusion of a “risk-of-use” trigger, the extent to which a federal standard would preempt state laws, and enumerating exceptions for different types of data make a single piece of federal legislation covering all instances of data breaches too unwieldy.²¹¹

A. *Federalism and Market-Based Equilibrium*

Businesses have a market-based incentive to create and abide by strong breach notification policies. The current state-based system emulates a marketplace, allowing the full array of tools for addressing data breaches to play out in a “robust test” for what the best solutions might be.²¹² Even so, it is not clear that a federal standard should be the ultimate goal. A market-based theory does not necessitate a clear “best” solution, but rather offers alternatives—different combinations of interests that serve different ends.²¹³ States as actors in a marketplace, however, need not imply that the result of competition is a race-to-the-bottom dilution of consumer protection.

209. Brendan St. Amant, Note, *The Misplaced Role of Identity Theft in Triggering Public Notice of Database Breaches*, 44 HARV. J. ON LEGIS. 505, 512–13 (2007) (noting that federal bills have “conflated the risk of harm with the risk of identity theft” and focus on preventing unauthorized financial transactions). By focusing on “data control” at the expense of other dignitary interests, the proposed federal breach laws enable citizens to take action only when a breach could result in financial harm. *See supra* Part III.B.

210. *See supra* Part II.A.

211. Picanso, *supra* note 23, at 385–86.

212. Flora J. Garcia, Comment, *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).

213. *See, e.g.*, Briffault, *supra* note 117, at 303 (“Different states may take different approaches—reflective of different local views—to the same problems.”).

Instead, a patchwork of laws of various stringencies and persuasions creates an environment in which businesses will compete to offer consumers additional protections where it is worthwhile to do so.²¹⁴ Some of the same tensions inherent in the consumer–business continuum explain the dynamics of a market-based approach to breach notification policy.²¹⁵ So far, an assumption of the federal data notification debate has been that the market will not respond to consumer demands for broader privacy protection without a regulatory framework to which consumers can hold corporations responsible.²¹⁶ Privacy advocates worry that companies think about data breaches from the perspective of “‘[b]ad press equals brand damage,’” not from the perspective of securing their customers against harm from misuse of their personally identifiable information.²¹⁷ But setting statute-based notification obligations aside, companies’ motivations to protect data and to notify when data is breached already stem from several sources.²¹⁸ A Ponemon Institute consumer survey on data breaches shows that consumers are generally dissatisfied with the notification process used by companies following a data breach affecting their personal information.²¹⁹ Fifty-seven percent said they lost trust and confidence in the organization, with thirty-one percent terminating their relationship with the organization.²²⁰ Companies that provided timely notification informing consumers of how to take advantage of free credit reporting services or other subsidized products, however, experienced

214. For instance, New York’s tough privacy laws, *see, e.g.*, N.Y. GEN. BUS. LAW § 899-aa (McKinney Supp. 2009), may press a data brokerage firm in Rhode Island to adopt a more robust data privacy policy when it would not be otherwise compelled. A weak federal law of the type proposed in Congress would level this field, disincentivizing businesses from voluntarily stepping up to stricter notification policies.

215. *See supra* Part I.B.

216. Nimmer, *supra* note 73, at 327–28 (“Data control policy posits that markets will not protect what the control advocate believes should be protected because corporations dominate and individuals are powerless without regulatory help.”).

217. Brenner, *supra* note 26 (quoting Christopher Barker, former Vice President and security team leader of Text 100).

218. Smedinghoff, *supra* note 1, at 22. Sources include common law obligations, rules of evidence, industry standards, contractual obligations, and self-imposed obligations. *Id.* at 24.

219. PONEMON INST., CONSUMERS’ REPORT CARD ON DATA BREACH NOTIFICATION 2 (2008), <http://www.idexperts.com/breach/ponemon-study/index.aspx> (extrapolating from study data the link between a bungled data breach notification campaign and a decline in customer confidence, loyalty, and retention). Somewhat ironically, users must provide some personal information in exchange for downloading the report. ID Experts, Registration Page, http://www.idexperts.com/breach/download/?altid=b_ponemon_study (last visited Nov. 9, 2009).

220. PONEMON INST., *supra* note 219, at 2.

much lower rates of customer “churn” and loss of consumer confidence.²²¹

Thus, there is a strong market-driven incentive for businesses to carefully consider data security and their own breach notification policies in addition to what the law might require. For example, by extending benefits to shoppers in exchange for discounts, or by promising heightened privacy measures to persuade clients to provide personally identifiable information, businesses link these programs to their own reputation.²²² A business “therefore has some incentive to police the actions of the parties to which it sells the data . . . because its interests are aligned with the interests of its customers.”²²³ The *Self-Regulatory Principles for Online Behavioral Advertising*, recently released by leading advertising industry groups, demonstrates that some businesses will respond to market shifts in consumer expectations.²²⁴ It should not matter what the companies’ motivations are for protecting consumer data if the end result is heightened protection.

To allow this interplay between consumer protection and business development, states will come to their own conclusions about the unique interests of their citizens and industries.²²⁵ This understanding provides support for those states that have chosen not to enact breach laws at all, which is a valid outcome under the four-factor framework when a state favors business interests to the exclusion of consumer protection.²²⁶ States are also poised to recalibrate the balance of interests as technology changes and risks shift.²²⁷ The countervailing force against states setting notification standards too low is the backlash from citizen–consumers. If states come down on the other extreme and enact excessive regulations,

221. *Id.*

222. *See* Deighton, *supra* note 104, at 144.

223. *Id.*

224. *See, e.g.*, AM. ASS’N OF ADVER. AGENCIES ET AL., SELF-REGULATORY PRINCIPLES FOR ONLINE BEHAVIORAL ADVERTISING (2009), available at <http://www.iab.net/media/file/ven-principles-07-01-09.pdf> (outlining consumer-friendly standards for the online collection and use of consumer data). Other self-regulatory programs include the TRUSTe privacy seal and “trustmarks.” TRUSTe, <http://truste.com/index.html> (last visited Nov. 1, 2009). Such seals and “trustmarks” are provided by McAfee Web Security Service. McAfeeSecure.com, <http://mcaffesecure.com/us/> (last visited Nov. 1, 2009).

225. Briffault, *supra* note 117, at 303.

226. *See supra* Part I.C.

227. For example, Missouri’s six-year resistance to a breach law gave way to a robust data breach notification law, which went into effect on August 28, 2009. MO. REV. STAT. § 407.1500 (West, Westlaw through 2009 First Regular Sess.); *see also supra* notes 132–35 and accompanying text.

companies have the protection of lobbying their local legislators (or even moving their offices to other states), rather than having to make their voice heard in Washington.²²⁸

Whether a state believes businesses are the right entities to make this notification determination is the sort of balancing between protecting consumers and promoting business that state legislatures are poised to do.²²⁹ The variables are many. The inclusion of risk-based notification exemptions²³⁰ permit a business to “avoid reporting entirely based on its own determination that the risk of misuse of the compromised information is low.”²³¹ Valuing consumer protection over business interests, a state might choose not to include a risk-based exception to breach notification in its statute. But disclosure of a breach when there is little or no risk of harm might create unnecessary concern and confusion.²³² Sending too many notices, based on overly strict criteria, could render all such notices less effective, because consumers could become desensitized to them and fail to act when risks are truly significant.²³³ On a national level (or even state level, for that matter), the optimal balance is far from clear. Instead, the current state-based system permits the market to suggest the point of equilibrium.²³⁴

By leaving states to craft notification law, the benefit is not only that more than fifty jurisdictions can test various solutions but also that businesses are free to compete to offer consumers ever stronger data and privacy protections.²³⁵ Given that notification laws’ effectiveness is still uncertain,²³⁶ a federal law could also lead to a false sense of security, underplaying the alternative solutions (such as

228. McCullagh, *supra* note 186.

229. *See, e.g.*, BOSSO ET AL., *supra* note 66, at 117; Chris Soghoian, *Indiana Passes Blogger-Written Data Breach Bill*, CNET NEWS, Mar. 25, 2008, http://news.cnet.com/8301-13739_3-9902569-46.html (discussing the willingness of Indiana State Representative Matt Pierce to listen to constituents in drafting and submitting a data breach notification bill to the state legislature).

230. *See supra* Part I.A.2.

231. Silverman, *supra* note 53, at 6.

232. U.S. GOV’T ACCOUNTABILITY OFFICE, REPORT TO CONGRESSIONAL REQUESTERS, PRIVACY: LESSONS LEARNED ABOUT DATA BREACH NOTIFICATION 2 (2007), available at <http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=gao&docid=f:d07657.pdf>.

233. *Id.*

234. *See, e.g.*, *New State Ice Co. v. Liebmann*, 285 U.S. 262, 311 (1932) (Brandeis, J., dissenting) (“[O]ne of the happy incidents of the federal system [is] that a single courageous State may, if its citizens choose, serve as a laboratory; and try novel social and economic experiments without risk to the rest of the country.”).

235. *See supra* note 214 and accompanying text.

236. *See supra* notes 23–24 and accompanying text.

standards for data protection) that states may prefer to impose.²³⁷ As for the burden on businesses to comply with many layers of laws, “[t]he cost of a breach in business lost and in goodwill tarnished is far greater than the costs of compliance with the various laws, which simply encourage good data practices and responsible treatment of consumers.”²³⁸ In fact, many large companies already profess to be experts in a state-based compliance program of sorts: advertising. “If large national companies can afford to market to individual consumers, as they increasingly claim to, they should be able to conform to slightly different laws in each state.”²³⁹

B. Preemption

Not only would a federal breach law likely stifle market-based innovation among states, the measures introduced so far in the 111th Congress would preempt existing state notification laws.²⁴⁰ As discussed above, this would hamper states’ ability to develop policy that balances the competing interests at stake in the sphere of data collection and security.²⁴¹ The proposed federal laws fail to address important questions of federalism, particularly whether and to what extent states would remain free to tailor their own regulations.²⁴² Preemption of consumer laws is generally not a good idea.²⁴³ “States should be allowed to offer their residents greater protections, and to experiment with new approaches.”²⁴⁴ A federal law that preempts state protections would erase the legislative process that, in some states, has taken years to get just right.

Some proponents of a federal law advocate legislation that contains very narrow preemption provisions, GLBA-style savings

237. For a discussion of various state data protection laws, see *supra* notes 136–41 and accompanying text.

238. Garcia, *supra* note 212, at 727. The commercial insurance industry has capitalized on the risks posed by data breaches to both consumers and businesses, because where actual damages are involved, the costs associated with managing a breach are fairly easily calculated: insurance companies are thus often willing to extend breach policies to insureds, reimbursing costs ranging from printing and mailing notification letters to fraud and identity theft services for victimized individuals. See, e.g., Goodman, *supra* note 30, at 19 (discussing insurance as an efficient solution to the data breach notification problem).

239. Matt Hines, *Debate Lingers over Federal Data-Handling Laws*, INFOWORLD, Apr. 3, 2007, <http://www.infoworld.com/t/business/debate-lingers-over-federal-data-handling-laws-357?page=0,1>.

240. Kennedy & Kennedy, *supra* note 5, at 25.

241. See *supra* Part I.B.

242. See, e.g., McCullagh, *supra* note 13.

243. Editorial, *Protecting Electronic Data*, N.Y. TIMES, May 25, 2009, at A18.

244. *Id.*

clauses, and exemptions for encrypted data or immaterial breaches.²⁴⁵ But this would, at best, add another layer of regulation onto the existing patchwork of statutes without clarifying anything, and, at worst, it would confound the prerogative that states have to define and protect the interests of their citizens and businesses.²⁴⁶ As shown in Part II.B above, any consensus that could be reached on a federal level is likely already covered by industry-specific laws.

“If Congress does pass a data security breach notification law . . . it is likely to be a weak version, with a risk-based exception and no private right of action. . . . Such a law would have the net effect of easing the compliance burden on businesses.”²⁴⁷ While states may currently provide a private right of action based on a dignitary, noneconomic theory of the privacy right discussed in Part I, the pending federal bills do not even broach the idea of nonpecuniary harm suffered by an individual whose data is leaked. Neither do the pending bills create a private, federal cause of action, and none gives rise to an action under state consumer protection laws for private individuals.²⁴⁸ Denying individuals a private right of action would strip standing to sue from a set of potential plaintiffs currently entitled to seek damages by the states permitting such suits. Federal legislation, as proposed, would therefore have the effect of undermining current consumer protections.²⁴⁹ “The examples are legion where industry says we need a national uniform law and that they will support one, and then Congress ends up passing a weak law full of exceptions that takes away state activities forever, and it’s not worth the price.”²⁵⁰ Where states have concerns about businesses’ ability to adequately protect consumers, preemption of more stringent state standards—standards deemed by a given state as necessary for consumer protection—leaves states and their citizens without recourse. As argued in Part IV.A above, this is a decision that states are better positioned than Congress to make—and fix, when necessary.²⁵¹

245. See, e.g., Picanso, *supra* note 23, at 389.

246. See *id.* at 370 (“Calls for federal legislation mandating adequate security measures for sensitive data are tempered by concerns that such legislation may water down existing state protections.”).

247. Silverman, *supra* note 53, at 10.

248. Kennedy & Kennedy, *supra* note 5, at 25–26.

249. Picanso, *supra* note 23, at 387.

250. Hines, *supra* note 239 (quoting Ed Mierzwinski, Consumer Program Director of the National Association of State Public Interest Research Groups (“U.S. PIRG”)).

251. See Briffault, *supra* note 117, at 303 (“State-level decision-making makes it possible for government to be more responsive to the diverse needs, preferences, and circumstances of our heterogeneous society.”).

C. Inflexibility

One of the greatest limitations of a federal standard is the lethargy with which it would respond to new challenges.²⁵² A federal law that aims to address the complex, multivariable definition of personally identifiable information, let alone the manner in which companies must respond to breaches, would not be nimble enough to remain relevant in a rapidly changing industry.²⁵³ With information security, legal standards recognize that “security is a moving target. Businesses must constantly keep up with every changing [sic] threats, risks, vulnerabilities, and security measures available to respond to them.”²⁵⁴ As privacy law in the electronic age anticipates rapid change, federal legislation is not likely to be flexible enough to keep pace with the evolution of technology. Indeed, at least one security expert has argued that even state laws are in danger of becoming obsolete in the face of new identity verification technologies.²⁵⁵ For example, advances in technology that enable encrypted data to be “deanonymized,” thereby reidentifying individuals thought to be secured within scrubbed records, could render any notification law with an encryption exception useless.²⁵⁶

Given that forty-five states have managed to pass breach notification laws since 2003 while federal equivalents have died in committee, the relative speed with which state and federal provisions could be amended to address new threats speaks for itself.²⁵⁷

CONCLUSION

Data breach notification laws are still in their infancy. Rather than subjecting businesses to federal blanket disclosure requirements, allowing the market to correct the data breach problem state-by-state

252. See Deighton, *supra* note 104, at 137 (“Rules lag behind the cunning of those who find new ways to exploit the limitations of the rules.”).

253. See St. Amant, *supra* note 209, at 515 (“[F]ederal laws are not well-suited to overseeing an increasingly complex and ever-changing industry.”).

254. Smedinghoff, *supra* note 1, at 53 (noting that effective regulatory data protection measures cannot be ensured by a particular product or a specific policy: review and adjustment are important considerations in any security framework).

255. See Oscherwitz, *supra* note 23.

256. See Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 U.C.L.A. L. REV. (forthcoming Aug. 2010) (forecasting the false sense of security that encrypted, redacted, or anonymized data may prove to lend).

257. See *supra* note 5 and accompanying text; see also Hines, *supra* note 239 (“States have always done a better job at protecting the privacy of their residents because they can act more quickly and decisively in creating and enforcing laws” (quoting Ed Mierwinski, consumer program director at U.S. PIRG)).

is the best way to ensure that the level of rigor is properly calibrated. The current state laws are already emulating such a market. “[A]nyone who supports the idea of increasing competition between corporations should like the idea of competition among different legal systems.”²⁵⁸ This is not to say that any given state’s statute “has it right.” This Comment does not argue that a breach notification law should lean more toward consumer protection or business interests, or that the scope of a law should encompass noneconomic harm. It does not even argue that states should pass breach notification statutes. This Comment does argue, however, that a federal law would cut off the market-driven process that is currently underway among the states.

While a blanket federal disclosure law would be too blunt a tool to take into account businesses’ own risk assessments, a set of guidelines, like those the Government Accountability Office has urged the Office of Management and Budget to develop for federal agencies, could assist businesses in making decisions as to when to offer more robust assistance or protection in the event of a breach.²⁵⁹ Companies can offer a range of services to their customers or clients to the extent feasible for that company, including informational Web sites, toll-free call-in numbers, identity theft insurance, assistance with implementing a credit freeze, or providing new account numbers or passwords.²⁶⁰ Furthermore, measures such as the GLBA and FACTA already provide security and notification procedures with respect to data elements that carry a high risk of being misused.²⁶¹ While there is now broad agreement that printing an individual’s full social security number on various documents is bad practice, there is no such consensus with respect to other data elements.²⁶²

More important, it is not clear that the end point of such a market-driven process should be a federal standard. In drafting statutes to address the problems that security breaches cause, states have undertaken several balancing acts to arrive at what they feel is the optimal solution in each of their jurisdictions. These decisions include determining whether there is more at stake than individual

258. McCullagh, *supra* note 186.

259. U.S. GOV’T ACCOUNTABILITY OFFICE, *supra* note 232, at 5.

260. Laudise, *supra* note 36, at 409.

261. *See supra* Part II.B.

262. *See, e.g.,* Nimmer, *supra* note 73, at 325 (“[V]oluntarily undertaken contractual obligations and market forces to define the scope of data control . . . should be displaced only when broad consensus exists that particular uses of the particular data should be restricted.”).

consumers' economic interests, specifically, whether there are broader privacy norms that are worth protecting through the mechanism of notification laws. Also at stake is the balance that must be struck in defining who, when, and how to notify—the balance between consumer protection and encouraging business within a state. These decisions are critical aspects of how states define interrelationships among stakeholders within their borders. Even assuming a federal law could capture the “best practices” proven through various state experiments, a uniform standard strips this defining power from states to set the bar at the level each finds fitting.

SARA A. NEEDLES