# FEDERAL SECURITY BREACH NOTIFICATIONS: POLITICS AND APPROACHES

*By Priscilla M. Regan*[†]

## TABLE OF CONTENTS



## I. INTRODUCTION

Proposals for a federal security breach notification law have been on the congressional agenda since 2005 when numerous bills on this topic were introduced in the 109th Congress. In subsequent sessions, Senate and House committees have approved bills and sent them to the full chamber. For example, House Bill 4791, which requires federal agencies to notify individuals



† Department of Public and International Affairs, George Mason University.

if their personally identifiable information was compromised or accessed during a security breach,[1] passed the House by a voice vote in June 2008.[2] No stand-alone general security breach notification legislation has yet passed Congress, although some sector specific efforts have met success, including one specific to health records included in the 2009 stimulus bill[3] and one specific to Veterans Administration records.[4]

This Article analyzes a number of factors that hamper easy congressional agreement on the appropriate response to security breaches in the context of notification legislation. In particular, the controversy surrounding federal preemption, the policy goals of security breach notifications, the effectiveness of notification as a policy technique, and the scope of notification have impeded congressional efforts to pass a comprehensive breach notification law. Additionally, the Article discusses features of the relevant congressional policy processes, including partisan viewpoints on the issue and overlapping committee jurisdictions, which have also contributed to the difficulties in achieving congressional passage of security breach notification legislation.

The Article begins in Part II with a brief explanation of the history of security breach notification as an issue of congressional concern. Part III considers the issue of security breach notification in the context of information privacy legislation, identifying ways in which proposed policy approaches are similar to and different from information privacy policies generally adopted in the United States. In Part IV, the Article addresses the factors likely to affect the substance of congressional deliberations as well as the processes of those deliberations. Finally, in Part V, the Article assesses the likelihood for passage of general security breach notification legislation in the near term.

---

1. Federal Agency Data Protection Act, H.R. 4791, 110th Cong. (2007) (requiring the Director of the Office of Management and Budget to develop best practices for agencies to follow in conducting privacy impact assessments).

2. The Library of Congress, http://thomas.loc.gov/cgi-bin/bdquery/z?d110:HR04791:@@@L&summ2=m& (last visited July 11, 2009) (summarizing the legislation and detailing the legislative history). The House of Representatives passed House Bill 4791 on June 3, 2008 by voice vote and then referred to the Senate Committee on Homeland Security and Governmental Affairs. *Id.*

3. American Recovery and Reinvestment Act of 2009, Pub. L. No. 111-5, Div. A., Title XIII, § 13402, 123 Stat. 260 (codified at 42 U.S.C.A. § 17932).

4. Title IX of the Veterans Benefits, Health Care and Information Technology Act of 2006, Pub. L. No. 109-461, 120 Stat. 3403 (codified in scattered sections of 38 U.S.C.) (requiring the Department of Veterans' Affairs to issue regulations requiring notice to veterans when a data breach with a "reasonable risk" of misuse of data occurs).

## II. EMERGENCE OF BREACH NOTIFICATION LEGISLATION AS A CONGRESSIONAL CONCERN

The need for a federal security breach notification law was made clear by a sequence of events involving large scale disclosures of personal data. A 2005 data security breach at ChoicePoint, a huge data broker with about 19 billion public and private records, placed the issue of security breach notifications on the congressional agenda.[5] The company disclosed in February, 2005 that it had sold the Social Security Numbers, addresses, and other personal data for approximately 145,000 people to impersonators of business owners.[6] This news was quickly followed by other similar disclosures of security breaches by the LexisNexis Group, Bank of America, and Citibank.[7] By the end of October, 2005, the Privacy Rights Clearinghouse had identified eighty data breaches in the previous eight months, involving the personal information of more than 50 million people.[8]

The scale of the problem and accompanying media attention, coupled with existing public and governmental concern about identity theft,[9] brought the breach issue to the attention of Congress beginning in 2005. When the problem of security breaches initially received congressional attention, there were three aspects of the issue that served to define the policy problem, and subsequently affected the politics of the issue.[10] These include: weaknesses in

---

5. Tom Zeller Jr., *Breach Points Up Flaws in Privacy Laws*, N.Y. TIMES, Feb. 24, 2005, at C1 [hereinafter Zeller, *Breach Points Up Flaws in Privacy Laws*].

6. *Id.*

7. Tom Zeller Jr., *Another Data Broker Reports a Breach*, N.Y. TIMES, Mar. 10, 2005, at C1 [hereinafter Zeller, *Another Data Broker Reports a Breach*]; Tom Zeller Jr., The Scramble to Protect Personal Data, N.Y. TIMES, June 9, 2005, at C1 [hereinafter Zeller, *The Scramble to Protect Personal Data*].

8. Privacy Rights Clearinghouse, A Chronology of Data Breaches, http://www.privacyrights.org/ar/ChronDataBreaches.htm (last visited June 4, 2009). Privacy Rights Clearinghouse continues to maintain this record of data security breaches with information available at: http://www.privacyrights.org/ar/ChronDataBreaches.htm.
*Id.*

9. Both the General Accountability Office (GAO) and the Federal Trade Commission (FTC) have a history of active interest in the issue of identity theft. *See*, *e.g.*, U.S. GEN. ACCOUNTING OFFICE, IDENTITY THEFT: PREVALENCE AND COST APPEAR TO BE GROWING, GAO-02-363 (2002); U.S. GEN. ACCOUNTING OFFICE, IDENTITY THEFT: GREATER AWARENESS AND USE OF EXISTING DATA ARE NEEDED, GAO-02-766 (2002); U.S. GEN. ACCOUNTING OFFICE, IDENTITY THEFT: SOME OUTREACH EFFORTS TO PROMOTE AWARENESS OF NEW CONSUMER RIGHTS ARE UNDERWAY, GAO-05-710 (2005); FTC Identity Theft website, http://www.ftc.gov/bcp/edu/microsites/idtheft/ (last visited June 1, 2009).

10. Public policy scholars have demonstrated that there are often a number of ways in which a policy problem can be defined and that the choice of a particular definition will then determine the interests that believe themselves to be affected by the policy, which then influences the politics surrounding that policy. *See*, *e.g.*, JOHN KINGDON, AGENDAS, ALTER-

the ways existing federal laws protected personally identifiable information; the diversity of data management practices contributing to data security breaches; and a state law in California that appeared effective in dealing with data security breaches.

First, the revelations about security breaches made clear that the existing set of federal laws governing personal information were ineffective both because they were framed in terms of sectors of the economy, and because their provisions for redress of grievances were cumbersome at best. Most relevantly, the Fair Credit Reporting Act of 1970, as amended various times including by the Fair and Accurate Credit Transactions Act of 2003, set rules for consumer credit agencies and bureaus, as well as consumers' access and rights with respect to their credit reports.[11] The Gramm-Leach-Bliley Act of 1999 established regulations and procedures for financial institutions,[12] although the definition of a financial institution was incomplete.[13] Additionally, a number of other sectoral rules set security standards for personally identifiable information but did not require security breach notification; these included the Health Insurance Portability and Accountability Act if medical records were involved,[14] and the Driver's Privacy Protection Act of 1994 if state driving records were compromised.[15] In all of these cases the burden to learn about possible misuses of personally identifiable information was on the individual who would likely only discover that his or her information had been compromised after a misuse occurred. And any redress of the harm took place after the fact.

This sectoral approach to the protection of personal information has been a cornerstone of the U.S. approach to information privacy, largely in response to individual industry arguments that their personal information

---

NATIVES AND PUBLIC POLICY 1-4 (1997); Theodore J. Lowi, *American Business, Public Policy, Case-Studies, and Political Theory*, 16 WORLD POLITICS 677, 677-15 (1964).

11. Fair Credit Reporting Act, Pub. L. No. 91-508 (codified as amended at 15 U.S.C. § 1681); Fair and Accurate Credit Transactions Act of 2003, Pub. L. No. 108-159, 117 Stat. 1952 (codified at 15 U.S.C. § 1681).

12. Gramm-Leach-Bliley Financial Modernization Act, Pub. L. No. 106-102, Title V, 113 Stat. 1338 (1999) (codified at 15 U.S.C. §§ 6801-6827).

13. Title V, § 509(3) (excluding from the definition of "financial institution" any entity subject to the jurisdiction of the Commodity Futures Trading Commission; the Federal Agricultural Mortgage Corporation or any entity operating under the Farm Credit Act of 1971; or other secondary market institutions).

14. Health Insurance Portability and Accountability Act, Pub. L. No. 104-191, 110 Stat. 1936 (1996) (codified in scattered sections of 29, 42, 16, 26 U.S.C.).

15. Drivers Privacy Protection Act of 1994, Pub. L. No. 103-322, Title XXX, § 300001, 108 Stat. 2099 (codified at 18 U.S.C. §§ 2721-2725).

needs and practices were unique and should not be uniformly regulated.[16] But in the wake of the 2005 security breaches, this feature of U.S. policy was roundly criticized. For example, an information security company executive noted that the patchwork of policies was too "industry-specific" and that the focus of regulation should be on the type of data rather than the industry.[17] As the executive stated, "A credit card number or Social Security number has the same importance, regardless of the industry handling it."[18]

Weaknesses in the sectoral approach were especially obvious in the retail area, which was not subject to any sector-specific law protecting consumers, but which collected and transferred vast and detailed amounts of personal data. Data breaches at T.J. Maxx and Marshalls, revealed in 2007, allowed hackers to access credit and debit card data, driver's license numbers, and names and addresses.[19] Security analysts pointed out that retailers tended to keep more data than was necessary and that senior managers often did not even know what data were being retained in systems based on old programming.[20] A senior counsel for the American Bankers Association noted that banks were then "left having to pay for the mistakes of retailers" to cover the costs associated with reissuing cards and for any losses as a result of fraud.[21] These gaps in sector-specific laws mean that the burden of security breaches is distributed unfairly on certain industries.

A second aspect of the security breach notification issue was that the diversity of data management practices highlighted the need for federal legislation. Organizations were using different mechanisms to transfer personally identifiable data. Examples range from the high tech, encrypted high-speed digital communication, to the low tech, unencrypted compact discs transported by couriers or delivery services.[22] The security breach at Citigroup in-

16. *See generally* PRIVACY PROTECTION STUDY COMM'N, PERSONAL PRIVACY IN AN INFORMATION SOCIETY (1977) (discussing the Commission's attention to private sector organizations' interest in keeping their records free from unreasonable government interference); PRISCILLA M. REGAN, LEGISLATING PRIVACY: TECHNOLOGY, SOCIAL VALUES AND PUBLIC POLICY (1995) (discussing the complexity of records-generating relationships in modern industry).

17. Zeller, *Breach Points Up Flaws in Privacy Laws, supra* note 6, at C1 (quoting Joseph Ansanelli, chief executive and co-founder of Vontu).

18. *Id.*

19. Ellen Nakashima, *Customer Data Breach Began in '05*, *Retailer Says*, WASH. POST, Feb. 22, 2007, at D1.

20. *Id.*

21. *Id.* (quoting Nessa Feddis).

22. *See*, *e.g.*, Dave Lenckus, *Spotlight: Information Security*, BUSINESS INSURANCE, May 21, 2007, at 13; Jonathan S. Ziss, *Commentary: Accidents Happen; Know Your Responsibilities When Client Data Goes Missing*, ACCOUNTING TODAY, April 14, 2008, at 6. *See generally* Identify Theft Resource Center, Data Breaches, http://www.idtheftcenter.org/artman2/publish/

volved tapes of unencrypted data, which is a particular security risk.[23] One data security executive, who provides services for federal agencies, pointed out that one of the reasons why data are transported on tapes and by trucks is that the sizes of the data files are too large to be transmitted over an organization's Internet connection and that the creation of secure, dedicated networks is very expensive.[24] Relatedly, the data storage practices of organizations vary widely and thus can make it relatively easy for hackers to gain access to databases containing sensitive personal information.[25] The range of data handling practices was so diverse that it was clear that policy specific to a practice or technology would not provide an appropriate target of policy any more than a particular sector would be an appropriate policy focus.

Finally, there was an existing California state law that was relatively effective in dealing with security breaches. The California law required all organizations, regardless of sector, who experienced a data breach to take positive action notifying the people whose information was compromised by the breach.[26] The California law focused congressional attention on notification as the appropriate policy response to a security breach because California already required this response. For example, after the 2005 breach, ChoicePoint was required by state law to inform the residents of California whose information was involved in its data breach and, after the incident received much publicity, also informed residents in other states.[27] The ChoicePoint incident generated interest in other states to pass laws similar to that in California, and provoked industry interest in a uniform federal law which would simplify their compliance with different requirements and standards in vari-

---

lib_survey/ITRC_2008_Breach_List.shtml (last visited July 3, 2009) (archiving articles from 2005-2009 on data security breaches containing detailed information on the range of security practices used by companies in storing and transferring personally identifiable information).

23. Zeller, *The Scramble to Protect Personal Data*, *supra* note 7, at C1.

24. *Id.* (quoting Anthony A. Caputo, chief executive of SafeNet, a provider of encryption technology for high-speed networks).

25. *Id.*

26. California Security Breach Notification Act, A.B. 700, 2002 Leg., (Cal. 2002) (codified at Cal. Civ. Code §§ 1798.29, 1798.82). The act requires that

> [a]ny person or business that conducts business in California, and that owns or licenses computerized data that includes personal information, shall disclose any breach of the security of the system . . . to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

*Id. See also* James F. Brelsford, *California Raises the Bar on Data Security and Privacy*, FINDLAW, Sept. 30, 2003, http://library.findlaw.com/2003/Sep/30/133060.html.

27. *See* Zach Patton, *Stolen Identities*, GOVERNING, Aug. 2005, at 39.

ous state laws.[28] The California law thus provided a model policy response to breaches—notification—and set the starting point for the policy deliberations in Congress and for similar conversations in other state legislatures.[29] As of June, 2009, forty-four states had passed a security breach notification law.[30]

Following the ChoicePoint incident, almost twenty bills involving security breach notifications were introduced in the House and the Senate in the 109th Congress.[31] In the first session, three congressional committees held hearings.[32] Senate committees passed three bills,[33] and a committee report was issued for one bill.[34] In the second session, House committees reported three bills,[35] with an effort to reconcile differences between two committee

28. The Business Software Alliance in May, 2005 proposed a federal security breach notification law as federal regulation that would prevent the development of "an onerous regulatory environment" that would likely result from various state laws. Patience Wait, *Industry Executives Ask for New Notification Law*, WASHINGTON TECHNOLOGY, May 18, 2005, http://washingtontechnology.com/Articles/2005/05/18/Industry-executives-ask-for-new-notification-law.aspx?Page=1; *see also* Jacob Freedman, *Industry Seeks One Law on Data Breach Alerts*, 64 CONG. Q. WKLY. REP. 314, 314 (describing how a uniform breach notification law has become one of the top priorities for banks and other financial companies); *cf.* CONSUMERS UNION, NOTICE OF SECURITY BREACH STATE LAWS (2007), http://www.consumersunion.org/campaigns/Breach_laws_May05.pdf (summarizing state laws as of August 2007).

29. Kathleen Hunter, *California law on ID theft seen as model*, STATELINE, Apr. 4, 2005, http://www.stateline.org/live/ViewPage.action?siteNodeId=136&languageId=1&contentId=22828.

30. Alabama, Kentucky, Mississippi, Missouri, New Mexico, and South Dakota are the only six states not to have done so. For a listing of the states and relevant legislation, see National Conference of State Legislatures, State Security Breach Notification Laws, http://www.ncsl.org/programs/lis/cip/priv/breachlaws.htm (last updated May 26, 2009).

31. GINA STEVENS, CONG. RESEARCH SERV., CRS REPORT NO. RL33273, DATA SECURITY: FEDERAL LEGISLATIVE APPROACHES 5-13 (2008) [hereinafter DATA SECURITY].

32. These included the Senate Committee on the Judiciary; the House Committee on Financial Services; and the Subcommittee on Commerce, Trade, and Consumer Protection of the Senate Committee on Energy and Commerce. *Id.* at 1 n.2.

33. Notification of Risk to Personal Data Act, S. 1326, 109th Cong. (2005) (reported by the Senate Judiciary Committee on October 20, 2005); Identity Theft Protection Act, S. 1408, 109th Cong. (2005) (reported by the Senate Commerce, Science and Transportation Committee on December 12, 2005); Personal Data Privacy and Security Act of 2005, S. 1789, 109th Cong. (2005) (reported by the Senate Judiciary Committee on November 17, 2005).

34. S. REP. NO. 109-203 (2005) (reporting on S. 1408).

35. Data Accountability and Trust Act (DATA), H.R. 4127, 109th Cong. (2005) (reported by House Committee on Energy and Commerce on May 4, 2006); Financial Data Protection Act of 2005, H.R. 3997, 109th Cong. (2005) (reported by House Financial Services Committee on May 4, 2006); Cyber-Security Enhancement and Consumer Data Protection Act of 2006, H.R. 5318, 109th Cong. (2006) (reported by House Committee on the Judiciary on June 22, 2006).

bills failing.[36] Additionally, the 109th Congress passed a law in response to the data breach by the Department of Veterans Affairs that compromised personal information on 26.5 million veterans.[37]

The issue of data security breaches returned to the congressional agenda in the 110th Congress. During the first session, Senate committees favorably reported three bills[38] and committee reports were issued for two bills.[39] During the second session, the House passed a bill, by voice vote and under suspension of the rules, which established new requirements on federal agencies and required the Office of Management and Budget (OMB) to notify individuals whose personal information may have been compromised or accessed during a government agency security breach.[40] Congressional action, and lack of action, underscored the difficulties of passing uniform legislation for security data breaches.

The 111th Congress adopted federal security breach notification requirements as part of the electronic health records stimulus provisions in the American Recovery and Reinvestment Act of 2009 (ARRA).[41] ARRA amended the Health Insurance Portability and Accountability Act of 1996 (HIPAA)[42]—through provisions in the Health Information Technology for Economic and Clinical Health Act (HITECH Act)—expanding the scope of the privacy and security requirements for health data and requiring hospitals, providers, and other HIPAA covered entities to implement security breach notification requirements.[43]

---

36. *See* DATA SECURITY, *supra* note 31, at 2.

37. Veterans Benefits, Health Care, and Information Technology Act of 2006, Pub. L. No. 109-461, 120 Stat. 3403. Title IX requires the Department of Veterans Affairs to issue regulations regarding notices to veterans when a data breach with "reasonable risk" for misuses of information occurs. *Id.*

38. Notification of Risk to Personal Data Act of 2007, S. 239, 110th Cong. (2007) (reported by Senate Committee on the Judiciary, May 31, 2007); Personal Data Privacy and Security Act of 2007, S. 495, 110th Cong. (2007) (reported by Senate Committee on Judiciary on May 23, 2007); Identity Theft Prevention Act, S. 1178, 110th Cong. (2007) (reported by the Senate Committee on Commerce, Science and Transportation, Dec. 5, 2007).

39. S. REP. NO. 110-70 (2007) (reporting on S. 495); S. REP. NO. 110-235 (2007) (reporting on S. 1178).

40. Federal Agency Data Protection Act, H.R. 4791, 110th Cong. (2007) (passed the House on June 3, 2008).

41. American Recovery and Reinvestment Act of 2009, Pub. L. No. 111-5, Div. A., Title XIII, § 13402, 123 Stat. 260 (codified at 42 U.S.C.A. § 17932).

42. Health Insurance Portability and Accountability Act, Pub. L. No. 104-191, 110 Stat. 1936 (1996) (codified in scattered sections of 29, 42, 16, 26 U.S.C.).

43. *See* Jeffrey D. Neuburger & Sara Krauss, Will Congress Enact Data Security Breach Provisions This Year? Guess What, It Already Has, Proskauer Rose LLP Privacy Law Blog, http://privacylaw.proskauer.com/2009/03/articles/security-breach-notification-l/will-

Under the HITECH Act, signed by President Obama on February 17, 2009, the covered entities must notify affected individuals when there is a security breach of unsecured "protected health information."[44] Moreover, the entities must inform Health and Human Services (HHS) and the media if the breach involves more than 500 individuals.[45] The HITECH Act pre-empts contrary state laws but leaves intact stronger state laws, rendering HITECH a floor for security breach notifications, not a ceiling.[46] It also authorizes state attorneys general to take action if they believe that an interest of State residents has been threatened by someone who violated HIPPA Privacy and Security rules.[47] The Act requires the Secretary of HHS to issue interim final regulations within 180 days of passage of the legislation, by August 17, 2009. HHS issued guidance on unsecured protected health information on April 17, 2009 with a public comment period open through May 21, 2009.[48] HITECH also requires the Federal Trade Commission (FTC) to develop temporary provisions applying to vendors of personal health records.[49] On April 20, 2009 the FTC issued a proposed rule open to public comment through June 1, 2009.[50]

The 111th Congress has also taken action on the Data Accountability and Trust Act (House Bill 2221), a bill first introduced in the 109th Congress,[51] following the 2005 ChoicePoint data breach discussed above, and reintro-

---

congress-enact-data-security-breach-provisions-this-year-guess-what-it-already-has/ (Mar. 2, 2009).

44. 45 C.F.R § 160.103 (2006); *see* Neuburger & Krauss, *supra* note 43.

45. American Recovery and Reinvestment Act of 2009, Pub. L. No. 111-5, Div. A., Title XIII, § 13402(e)(3), 123 Stat. 260 (codified at 42 U.S.C.A. § 17932).

46. *Id.* § 13421(a); *see also* Neuburger & Krauss, *supra* note 43.

47. *Id.* § 13410(e)(1). Prior to passage of the HITECH Act, the Secretary of Health and Human Services was the only person authorized to pursue civil enforcement for HIPPAA's Privacy and Security rules. *See* GINA STEVENS & EDWARD C. LIU, Cong. Research Serv., CRS Report No. R40546, THE PRIVACY AND SECURITY PROVISIONS FOR HEALTH INFORMATION IN THE AMERICAN RECOVERY AND REINVESTMENT ACT OF 2009, at 18 (2009).

48. Guidance Specifying the Technologies and Methodologies That Render Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals for Purposes of the Breach Notification Requirements, 74 Fed. Reg. 19,006 (Apr. 27, 2009) (to be codified at 45 C.F.R. pt. 160, 164).

49. American Recovery and Reinvestment Act of 2009, Pub. L. No. 111-5, Div. A., Title XIII, § 13407(g)(1), 123 Stat. 260 (codified at 42 U.S.C. § 17932).

50. Health Breach Notification Rule, 74 Fed. Reg. 17,914 (Apr. 20, 2009) (to be codified at 16 C.F.R. pt. 318); *see* Bureau of National Affairs, *FTC Issues Proposal on Consumer Notice for Breaches of Electronic Health Information*, HEALTH PLAN & PROVIDER REP., Apr. 22, 2009, http://healthcenter.bna.com/pic2/hc.nsf/id/BNAP-7RCKMD?OpenDocument&Print Version=Yes.

51. Data Accountability and Trust Act (DATA), H.R. 4127, 109th Cong. (2005) (placed on the Union Calendar on June 2, 2006).

duced in the 110th Congress.[52] House Bill 2221 would establish uniform requirements for businesses to notify individuals when an unauthorized party had access to personally identifiable information as a result of a security breach.[53] Hearings on this bill, sponsored by Representative Bobby Rush, were held on May 5, 2009 by the Commerce, Trade, and Consumer Protection Subcommittee of the House Energy and Commerce Committee. On June 3, 2009 the subcommittee forwarded an amended version of the bill to the full committee for its consideration.[54]

## III. A TYPICAL CASE OF INFORMATION PRIVACY POLICY?

The definition and formulation of policies regarding security breach notifications appears in several respects to be similar to earlier information privacy policies, although there are some important differences. This Part considers these similarities and differences as they relate to the definition of the problem of security breaches, the proposed solution of notification, and the politics of congressional deliberations.

### A. SIMILARITIES TO OTHER PRIVACY ISSUES

The emphasis on notices as a solution follows in the tradition of fair information principles that were first developed in 1973 by the Department of Health, Education and Welfare's Advisory Committee on Automated Personal Data Systems.[55] These principles have become the standard legislative and organizational response to the privacy of personally identifiable informa-

52. Data Accountability and Trust Act, H.R. 958, 110th Cong (2007) (referred to the House Subcommittee on Commerce, Trade and Consumer Protection of the Committee on Energy and Commerce on February 9, 2007 but no further action was taken).

53. Data Accountability and Trust Act, H.R. 2221, 111th Cong (2009).

54. The Library of Congress, http://thomas.loc.gov/cgi-bin/bdquery/z?d111:HR02221:@@@X (last visited July 23, 2009) (detailing the legislative history).

55. U.S. DEPT. OF HEALTH, EDUCATION & WELFARE, RECORDS, COMPUTERS, AND THE RIGHTS OF CITIZENS: REPORT OF THE SECRETARY'S ADVISORY COMMITTEE ON AUTOMATED PERSONAL DATA SYSTEMS, at xx-xxi (1973). The five basic principles include:

> There must be no personal record-keeping system whose very existence is secret. There must be a way for an individual to find out what information about him is in a record and how it is used. There must be a way for an individual to prevent information about him that was obtained for one purpose from being used or made available for other purposes without his consent. There must be a way for an individual to correct or amend a record of identifiable information about him. Any organization creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take precautions to prevent misuse of the data.

*Id.*

tion, enshrined in privacy laws in many countries and in standard privacy statements on organizational websites and written materials.[56] Notice is the primary way in which individuals learn of the existence of data systems and the information handling practices of those systems. Such notices are consistent with a governance strategy that Sunstein terms "regulation through disclosure"[57] and Fung, Graham and Weil (Fung et al.) term "targeted transparency."[58] Fung et al. argue that the fundamental idea of such transparency "was not just the public deserved better information . . . [but] that the power of information would create a chain reaction of new incentives."[59] They also point out what has been long recognized by privacy scholars as a problem with notices as a method of informing individuals about the personal information practices of various organizations.[60] Targeted transparency policies can do "more harm than good" as the "political compromise" by which they are formulated is often the product of "incomplete, inaccurate, obsolete, confusing, or distorted" information.[61] However, there are also circumstances under which targeted transparency can be effective; this will be discussed later in Part IV of the Article.

The issue of security breaches is also similar to the policy processes associated with other information privacy legislation in that it is incident or crisis driven. As discussed above, security breach incidents revealed by the media and various public interest groups put pressure on policymakers to respond. Incidents have provided the catalyst for a range of previous privacy laws including the Privacy Act of 1974,[62] the Family Educational Rights and Privacy Act of 1974,[63] the Right to Financial Privacy Act of 1978,[64] the Video Privacy Protection Act of 1988,[65] and the Driver's Privacy Protection Act of 1994.[66]

---

56. Robert Gellman, *A Better Way to Approach Privacy Policy in the United States: Establish a Non-Regulatory Privacy Protection Board*, 54 HASTINGS L. J. 1183, 1185 (2003).

57. Cass R. Sunstein, *Informational Regulation and Informational Standing: Akins and Beyond*, 147 U. PA. L. REV. 613, 613 (1999) (exploring the intersection between the law of standing and our regulatory regime mandating public disclosure).

58. ARCHON FUNG ET AL., FULL DISCLOSURE: THE PERILS AND PROMISE OF TRANSPARENCY 2, 5 (2007).

59. *Id.* at 2.

60. *Id.* at 7-10. *See generally* REGAN, *supra* note 16; Gellman, *supra* note 56.

61. FUNG ET AL., *supra* note 58, at 7.

62. Privacy Act of 1974, Pub. L. No. 93-579, 88 Stat. 1896 (codified at 5 U.S.C. § 552a).

63. Family Educational Rights and Privacy Act of 1974, Pub. L. No. 93-380, 88 Stat. 484 (codified at 20 U.S.C. § 1232).

64. Right to Financial Privacy Act of 1978, Pub. L. No. 95-630, 92 Stat. 3641 (codified at 12 U.S.C. § 3401).

65. Video Privacy Protection Act of 1988, Pub. L. No. 100-618, 102 Stat. 3195 (codified at 18 U.S.C. § 2710).

In each of these cases, anecdotes and media attention were critical to building public support and congressional pressure to take action.[67] Although there are shortcomings associated with such reactive policymaking,[68] it has indeed been the norm for information privacy legislation.

Because proposals for security breach notifications occurred as reactions to breaches and because the solutions were framed in terms of notices, both privacy advocates and those opposed to legislation viewed the issue through the conceptual lens of previous information privacy proposals.

### B. DIFFERENCES FROM OTHER PRIVACY ISSUES

However, there were four key differences between the issue of data breach notification and earlier privacy issues: security, rather than privacy, became the dominant framework defining the problem; proposed solutions put the burden on organizations rather than individuals; harmed individuals were seen as a socially situated group; and proposed solutions treated all organizations similarly. Each of these differences affected congressional deliberations and is discussed briefly below.

Unlike other information privacy issues, the issue of data breach notification is defined primarily in terms of security rather than privacy. Although information privacy and information security have often been recognized as two sides of the same coin, in the United States, privacy has been the more prevalent paradigm for considering policy responses to problems involving personal information.[69] Framing the issue of data breaches in terms of "security" places the emphasis not on normative or tangible harms to individuals but instead on organizational practices. The organization is the evident cause of the problem and the target of legislation. Organizational practices provide

---

66. Driver's Privacy Protection Act of 1994, Pub. L. No. 103-322, 108 Stat. 1796 (codified at 18 U.S.C. §§ 2721-2725).

67. For example, the adoption of the Video Privacy Protection Act followed a Washington D.C. paper's publication of a list of the videotapes rented by Robert Bork, then a nominee for the Supreme Court. *See* REGAN, *supra* note 16, at 199.

68. *See generally* COLIN J. BENNETT, REGULATING PRIVACY: DATA PROTECTION AND PUBLIC POLICY IN EUROPE AND THE UNITED STATES (1992) (describing how the United States' sectoral approach to privacy requires the formation of new coalitions and political conditions to legislatively address each new issue); DAVID FLAHERTY, PROTECTING PRIVACY IN SURVEILLANCE SOCIETIES: THE FEDERAL REPUBLIC OF GERMANY, SWEDEN, FRANCE, CANADA, AND THE UNITED STATES (1989) (describing how the lack of a permanent data protection framework in the U.S. has meant legislative policy responses to privacy issues are uncoordinated); REGAN, *supra* note 16 (describing how historically privacy issues have been on the congressional agenda for years and sometimes decades before Congress acts).

69. *E.g.*, REGAN, *supra* note 16, at 3 (explaining how the goal of protecting individual privacy has dominated policy debates around information security policy).

the focus for policy debate. And the focus of organizational practices is shifting as "PDAs, laptops and other mobile devices enable employees and others to remove data from the hardened interior, thus negating perimeter defenses."[70] This focus on security does not imply that privacy will be absent from the debate, but the shift in emphasis to security will affect both policy deliberations and what is believed to be an appropriate policy response.

A second difference from traditional information privacy issues is that proposed solutions put an affirmative requirement on organizations to respond to their security breaches by enhancing the care with which they handle personally identifiable information rather than by requiring them to provide broad notice to individuals. In general, the solution of security breach notification evaluates the effectiveness of an organization's security less on the basis of specific security practices, and more on the basis of how well the data is protected, or the results of those practices.[71] Security breach notification policies often provide organizations with discretion to adopt security practices that are most suited to their business model and information needs, but if those practices do not prevent security breaches, then notification of affected individuals is required.[72] The burden and cost of legislation is on the organization. This will likely shift the policy debate from the organization to the individual, as organizations will likely seek to minimize the costs on them and instead attempt to transfer those costs to individuals affected.

A third difference is that with security breaches, the proposed solution of notice is directed to the affected data subjects as a socially situated group who have had a similar experience. Because the individuals are notified as a result of harm to them as a group, the notice is likely to be more meaningful and timely, and there is a higher likelihood that affected individuals will pay attention. Perhaps more importantly, group notice emphasizes the social harm that has occurred as a result of the security breach. A security breach affects the relationship between an organization and a group associated with that organization, and therefore, the larger society has some legitimate claim to be informed of the breach. In many states and in some proposed federal legislation, notice is required not only to the group of affected individuals,

---

70. Dennis Hoffman & Ken Tyminski, *From Financial Services CISO to Chief Information Management Office: Tackling 360 Degrees of Enterprise Protection*, WALL ST. & TECH., April 26, 2007, *available at* http://www.wallstreetandtech.com/showArticle.jhtml?articleID=199201960.

71. David L. Silverman, *Data Security Breaches: The State of Notification Laws*, 19 NO. 7 INTELL. PROP. & TECH. L.J. 5, 5-12 (2007).

72. *Id.*

but must also be posted on an organization's website and revealed to a government entity and to the media.[73]

A final difference from other information privacy issues is that current policy proposals treat all organizations similarly, as opposed to the historical sectoral approach. Such an omnibus approach has not been typical in the United States, largely because organizations have lobbied that they have different information needs and practices, as well as different relationships with individuals, and thus should be treated differently.[74] In the case of security breaches, the harm to be corrected is that personally identifiable data has been compromised. As reflected in current proposals, this type of harm does not entail an analysis of the relationship of the individual to the organization or an understanding of the information needs of the organization. Such factors are not relevant because unauthorized release, theft, or loss of information is the common problem regardless of the type of relationship the data subject has with the organization experiencing the security breach.

## IV. POLICY AND PROCEDURAL OBSTACLES TO A UNIVERSAL BREACH NOTIFICATION LAW

Although the issue of security breaches and the policy solution of breach notifications arrived relatively recently on the congressional agenda, it is not too soon to analyze congressional deliberation thus far and to identify substantive areas that have caused disagreement and will require resolution for passage of any legislation. This Part will first consider several procedural factors which have historically complicated congressional processes and then examine relevant substantive issues.

### A. PROCEDURAL FACTORS

The issue of security breaches touches all organizational sectors, and therefore, bills designed to broadly address all sectors will be referred to multiple congressional committees. In the 109th Congress, eight congressional committees had jurisdiction over data security, data breach notification, and data privacy. On the Senate side, three committees had jurisdiction: Banking,

73. For example, the New York breach notification law requires notification to affected New York residents, the state attorney general, consumer protection board, and New York Office of Cyber Security and Critical Infrastructure Coordination, as well as to national consumer reporting agencies if the breach involves more than 5,000 New York residents. Erika S. Koster & Aaron Scott, *Breach and Tell: Security Breach Notification Laws*, THE COMPUTER & INTERNET LAWYER, March 2006, at 5. The North Carolina law similarly requires notification to the Consumer Protection Division of the attorney general's office and all national consumer reporting agencies. *Id.*

74. *See supra* note 16.

Housing, and Urban Affairs; Commerce, Science, and Transportation; and Judiciary.[75] On the House side, five committees had jurisdiction: Energy and Commerce; Financial Services; Government Reform; Judiciary; and Ways and Means.[76] A similar lineup of committees was involved in the 110th Congress and is likely to be involved in the 111th Congress. With such a combination, jurisdictional disputes are likely to occur. For example, in the 110th Congress, Senator Jeff Sessions took the position with respect to the Personal Data Privacy and Security Act of 2007, Senate Bill 495, that "some of the items that [Senate Bill] 495 addresses fall within the jurisdiction of the Senate Banking Committee, and are inappropriate topics for Senate Judiciary Committee legislation."[77] In 2006, a "turf war" occurred between the House Financial Services Committee, supporting House Bill 3997, and the House Energy and Commerce Committee, supporting House Bill 4127.[78] Each committee stripped the other committee's version of a security breach and data privacy bill and substituted its own committee's version, making it more unlikely that action on the House floor would be successful.[79]

Another procedural factor, related to the breadth of committee jurisdiction on privacy issues, is that members of Congress have taken differing approaches in drafting proposed legislation, which complicates the lawmaking process. Some members have approached the issue of security breaches as a new area for legislation and have drafted stand-alone bills,[80] while other members have framed their bills as amendments to existing legislation.[81] For example, several bills amend the Gramm-Leach-Bliley Act and require financial institutions to notify customers, consumer reporting agencies, and federal authorities when there is a breach.[82] Other bills take the approach of amending the Fair Credit Reporting Act to establish data security standards.[83] Another approach is to amend the Racketeer Influenced and Corrupt Organ-

75. DATA SECURITY, *supra* note 31, at 1.

76. *Id.*

77. S. REP. NO. 110-70 (2007), at 26.

78. Seth Stern, *House Panels Move Competing Data Privacy Bills After Text Swap*, 64 CONG. Q. WKLY. REP. 1484, 1484 (2006).

79. *See id.* Both were subsequently sent to the House floor but were not considered. The Library of Congress, http://thomas.loc.gov/cgi-bin/bdquery/z?d109:h.r.03997: (last visited July 23, 2009) (detailing the legislative history of HR 3997); The Library of Congress, http://thomas.loc.gov/cgi-bin/bdquery/z?d109:h.r.04127: (last visited July 23, 2009) (detailing the legislative history of HR 4127).

80. *See*, *e.g.*, Notification of Risk to Personal Data Act of 2005, S. 115, 109th Cong. (2005).

81. DATA SECURITY, *supra* note 31, at 5-13.

82. *See*, *e.g.*, Financial Privacy Breach Notification Act of 2005, S. 1216, 109th Cong. (2005).

83. *See*, *e.g.*, Financial Data Protection Act of 2005, H.R. 3997, 109th Cong. (2005).

izations Act.[84] Still others amend the Federal Criminal Code to prohibit unauthorized access to computer files or passwords, and to punish concealment of security breaches.[85] Not surprisingly, several bills amend more than one piece of existing legislation. The range of legislative approaches makes it more challenging to craft a consensus approach because sponsors and co-sponsors have voiced differing policy approaches in their own bills.

A third procedural factor is the partisan politics associated with congressional consideration of issues involving business regulation generally, including the issue of security breach notification. Democratic members of Congress were first to initiate legislative action in response to the 2005 ChoicePoint data security breach[86] and the 2006 theft of a government laptop from the home of a Veterans Affairs employee.[87] Although some bills have been co-sponsored by Democrats and Republicans, something of a party-line position seems to have emerged in several debates at the committee level.[88] Republicans often seem reluctant to impose what are viewed as burdens on companies for what is regarded as less than clear benefits for consumers who may be subject to over-notification.[89] Democrats, on the other hand, want regulators, and not companies, to decide when companies need to notify consumers of a security breach[90] and are opposed to federal legislation that would pre-empt the strong standards in state legislation.[91] A 2005 debate and party line vote in the House Energy and Commerce Subcommittee on Commerce, Trade, and Consumer Protection well illustrates the partisan differences.[92] Democrats criticized the Republican supported bill for containing too many loopholes, using a lax standard for when notification is required, preventing state attorneys general from assuming an enforcement role, and

84. *See*, *e.g.*, Personal Data Privacy and Security Act of 2005, S. 1789, 109th Cong. (2005).

85. *See*, *e.g.*, Personal Data Privacy and Security Act of 2007, S. 495, 110th Cong. (2007).

86. Seth Stern, *Data Brokers Scramble to Limit Regulation*, 63 CONG. Q. WKLY. REP. 881, 882 (2005).

87. Rebecca Adams, *Turning the VA's Loss Into Political Gain*, 64 CONG. Q. WKLY. REP. 1601, 1601 (2006).

88. *See*, *e.g.*, Amol Sharma, *Data Security Bill Approved Over Democrats' Objections*, 63 CONG. Q. WKLY. REP. 2998, 2998 (2005); Adams, *Supra* note 87 at 1601-02.

89. Alabama Republican Jeff Sessions noted during the November 2006 Senate Judiciary Committee's markup of an identity theft bill that "[n]otices can come so often that we become numb to them." Seth Stern, *Identity Theft Bills Offer Choices*, 64 CONG. Q. WKLY. REP. 1032, 1032 (2006).

90. Sharma, *supra* note 88, at 2998.

91. Michael R. Crittenden, *Bill Sets Standard for Data Security*, 64 CONG. Q. WKLY. REP. 775, 775 (2006).

92. Sharma, *supra* note 88, at 2998.

preempting stronger state laws.[93] Similarly, in 2006 several Democratic members of the House Financial Services Committee preferred the stronger and more comprehensive security breach notification requirements in the House Energy and Commerce bill over their own committee's bill.[94]

The President, the OMB, and the FTC have also joined policy discussions at the federal level, providing an alternative forum for policymaking which could lessen the perceived need for congressional action as incremental policy changes can occur through those processes.[95] In May 2007, the OMB issued a directive to federal agencies giving them 120 days to define their notification policies ,[96] which was issued in response to a report, "Combating Identity Theft: A Strategic Plan,"[97] submitted to the President by the President's Identity Theft Task Force.[98] The FTC, primarily using powers granted to it under the Gramm-Leach-Bliley Act, has been somewhat more active in taking actions against financial institutions, including retailers, who have not adequately protected customer information. For example, in 2005 the FTC settled with BJ Wholesale Club and with DSW because the two retailers were not providing effective security for customer records.[99]

These procedural issues involving questions of competing and overlapping congressional committee jurisdictions, the range of available legislative approaches to legislation, partisan differences on government regulation of business and the appropriate government role in the area of security breaches, and the involvement of other policy actors set the stage for consideration of specific substantive questions.

### B. SUBSTANTIVE POLICY ISSUES

In addition to procedure, debates about policy content are critical in congressional deliberations and in determining the likelihood that any legislation passes. At least four substantive issues have been the focus of congressional

---

93. *See* Jonathan Krim, *Parties Split on Data-Protection Bill*, WASH. POST, Nov. 4, 2005, at D04.

94. Stern, *supra* note 78, at 1484.

95. Jacqueline Emigh, *Tackling Identity Theft*, GOV'T SECURITY, Aug. 1, 2007, at 6.

96. Memorandum, Office of Mgmt. & Budget, Exec. Office of the President, Safeguarding Against and Responding to the Breach of Personally Identifiable Information OMB M-07-16, (May 22, 2007).

97. PRESIDENT'S IDENTITY THEFT TASK FORCE, COMBATING IDENTITY THEFT: A STRATEGIC PLAN (2007), http://www.idtheft.gov/reports/StrategicPlan.pdf.

98. The President's Identity Theft Task Force was created in 2006 to develop a strategic plan for the federal government to combat identity theft. Exec. Order No. 13,402, 71 Fed. Reg. 27,945 (May 10, 2006).

99. Jason Krause, *Stolen Lives*, 92 A.B.A. J. 36, 39-40 (2006).

debates thus far and are likely to remain hurdles to any legislative success on a breach notification law.

*1. Federal Preemption*

Policy conflicts and political alliances around the issue of security breach notification must be understood in the context of federalism. The passage of security breach notification legislation in California in 2002[100] reflects what federalism scholars have referred to as a recent upsurge in state government policy activism.[101] Dale Krane, for example, identifies several motivations that states have to pursue policy independently of the federal government: to fill a policy void that the federal government has chosen to not fill, to correct or modify perceived defects in federal policy, and to signal problems to the federal government.[102] In the wake of the 2005 ChoicePoint security breach, California's law requiring notification to affected individuals was widely perceived as an effective solution.[103] It was the only state with such legislation, and other states quickly followed California's example in passing similar laws.[104] By early 2006, twenty states had enacted security breach notification legislation.[105] By June, 2009, forty-four states had passed security breach notification laws, largely modeled on California's.[106]

Congressional consideration of the issue raised the fundamental question of whether federal legislation would weaken existing state requirements, eliciting a strong reaction among the states. Ed Mierzwinski, director of consumer programs for U.S. Public Interest Group, commented generally that the federal effort represented "another arrogant piece of federal legislation that proposes to strip states of their role as laboratories of democracy and hand corporations a huge giveaway."[107] In October, 2005, "47 state attorneys general sent a letter to Congress urging the creation of a tough, far-reaching

100. A.B. 700, 2002 Leg. (Cal. 2002) (codified at Cal. Civ. Code §§ 1798.29, 1798.82).

101. *See generally* John Dinan, *The State of American Federalism 2007–2008: Resurgent State Influence in the National Policy Process and Continued State Policy Innovation,* 38 PUBLIUS 381 (2008) (summarizing a variety of recent state efforts implementing state policies and influencing national policy-making ).

102. Dale Krane, *The Middle Tier in American Federalism: State Government Policy Activism During the Bush Presidency*, 37 PUBLIUS 453, 462 (2007).

103. Erika S. Koster & Aaron Scott, *Breach and Tell: Security Breach Notification Laws*, COMPUTER & INTERNET LAW., March 2006, at 1, 2; Silverman, *supra* note 71, at 5.

104. Hunter, *supra* note 29.

105. Koster & Scott, *supra* note 103, at 2.

106. The only states with no security breach law are Alabama, Kentucky, Mississippi, Missouri, New Mexico, and South Dakota. *See* National Conference of State Legislatures, *supra* note 30.

107. Kavan Peterson, *States Failing to Secure Personal Data*, STATELINE, July 12, 2006, http://www.stateline.org/live/details/story?contentId=126215.

bill."[108] States rights proponents and consumer advocates were also opposed to a national law that would preempt stronger state laws; as California State Senator Joe Simitian, the author of the California breach legislation, put it, "Let's not sacrifice the standard set in California on the altar of federal regulation."[109]

Many members of Congress are quite aware of the industry push to weaken state laws through federal preemption. In 2006, Barney Frank, the ranking Democrat on the House Financial Services Committee, said, "Whenever [the business community] feels threatened by the energy level of the states, then they come here and get pre-emption."[110] On the other hand, congressional supporters of federal preemption argued in the Financial Services Committee in 2006 that "'rogue' state governments could abuse" a law that gave them an active role in consumer notification.[111] In general, proponents of federal preemption believe that uniform standards are necessary to avoid confusion for industry and consumers.[112] Industry decries the "patchwork of state laws," arguing instead for a "uniform system across state lines" that "temper[s] mass notifications with an assessment of the actual risk that personal information will fall into the hands of data pirates."[113]

*2. Policy Goal*

To successfully enact federal breach legislation, the policy goal(s) to be achieved must be agreed upon, requiring an understanding of the problem being addressed.

If the problem is, as many have argued, reducing identity theft, then the focus is to determine the scope of identity theft, its causes, and an analysis of whether proposed alternatives effectively address those causes. The issue of identity theft has been of concern to the FTC, GAO, several congressional committees, and numerous interest groups since the 1990s. In 1998, Congress passed the Identity Theft and Assumption Deterrence Act, which made it illegal to steal another individual's personal information with the intent to make use of that information in a fraudulent manner.[114] The law established

108. Tom Zeller Jr., *Data Security Laws Seem Likely, So Consumers and Businesses Vie to Shape Them*, N.Y. TIMES, Nov. 1, 2005, at C3.

109. Jon Swartz, *Tech Experts Plot to Catch Identity Thieves; Politicians to Security Gurus Offer Ideas to Prevent Data Breaches*, U.S.A. TODAY, Feb. 9, 2007, at 7B.

110. Crittenden, *supra* note 91, at 775 (brackets in original).

111. *Id.*

112. Joe Hutnyan, *Moves to Toughen Data Theft Bill Put Pressure on Industry*, SEC. WK, Nov. 14, 2005, at 1.

113. Freedman, *supra* note 28, at 314.

114. Identity Theft and Assumption Deterrence Act of 1998, Pub. L. No. 105-318, 112 Stat. 3007.

that the victims of identity theft were the individuals whose identity was stolen, not the companies that lost money, and charged the FTC with establishing a clearinghouse and educating consumers.[115] The issue of identity theft has remained on the congressional agenda since the 1990s, with for example, seventeen bills introduced in the 107th Congress.[116] Identity theft provided a logical frame of reference for policy deliberations about security breach notifications because it was a prominent part of the ongoing policy discussions about the security of personally identifiable information and because the personal costs were tangible. Several security breach notification bills contained identity theft in their titles, and congressional hearings cast security breach notification as an "innovative solution" for the evolving problem of identity theft.[117] Congressional Research Service (CRS) reports[118] and media coverage[119] also linked identity theft and security breach notification, publicizing this connection.

If the policy problem is defined not as reducing identity theft but as correcting lax or ineffective organizational data security, then the policy goal of legislation is to improve data security practices. For some time, observers have pointed out that organizations tend to underestimate the intricacies of data security, and consequently under-invest in security protections.[120] Since data subjects do not "see" the value of data security protections, they do not demand those protections. If there has not been a costly security breach, then organizations do not have incentives to incur preventative security en-

115. *Identity Theft: Hearing Before the H. Comm. on Banking and Financial Services*, 105th Cong. (2000) (statement of Betsy Broder, Asst. Director for the Division of Planning and Information of the Bureau of Consumer Protection, FTC), *available at* http://www.ftc.gov/os/2000/09/idthefttest.htm (summarizing the law and the role of the FTC).

116. ANGIE A. WELBORN, CONG. RESEARCH SERV., CRS REPORT NO. RL 31752, IDENTITY THEFT: AN OVERVIEW OF PROPOSED LEGISLATION IN THE 107TH CONGRESS (2003) (listing and describing "Senate Bills: S. 848, S. 1014, S. 1399, S. 1723, S. 1742, S. 2541, S. 3100, House Bills: H.R. 220, H.R. 1478, H.R. 2036, H.R. 3053, H.R. 3368, H.R. 4513, H.R. 4678, H.R. 5424, H.R. 5474, H.R. 5588").

117. *See, e.g.*, *Identity Theft: Innovative Solutions for an Evolving Problem: Hearing before the Subcomm. on Terrorism, Tech., and Homeland Sec. of the H. Comm. on the Judiciary*, 110th Cong. (2007) [hereinafter *Hearing*].

118. DATA SECURITY, *supra* note 31, at 1 ("Because concerns about possible identity theft resulting from data breaches are widespread, Congress spent a considerable amount of time in the 109th Congress assessing data security practices and working on data breach legislation that would require companies to safeguard sensitive personal data and notify consumers about data security breaches.").

119. *See, e.g.*, Stern, *supra* note 78, at 1484; *Special Report: Identity Theft Prevention*, CONG. Q. WKLY. REP. 2324, 2324 (2005).

120. *See, e.g.*, Jacques S. Gansler & William Lucyshyn, *Improving the Security of Financial Management Systems: What are We to Do?*, 24 J. ACCT. & PUB. POL'Y 1, 4 (2005).

hancements. Many organizations "get by" with more minimal protections.[121] In effect, when left to its own devices, the "market" under-supplies security for data. Security breach notifications can be viewed as a mechanism for correcting that market imperfection by bringing to the organization's attention the cost of not adequately protecting data.[122]

Alternatively, the problem can be defined as lack of public awareness about the ways in which personally identifiable information is collected, exchanged, or retained.[123] In this view, the problem is that the public does not know about something that it arguably has a "right to know" about, and again the existing market and organizational incentive structure do not provide sufficient information for the public. This information asymmetry affects not only individuals' ability to protect themselves, but also, as Stacey Schreft points out, the public good of payment system integrity and efficiency.[124] One important component of personal information flows that has received more widespread attention, in part resulting from the existing state notification laws, is that a range of organizations handle and exchange personally identifiable information. Individuals themselves often do not have a direct relationship with these organizations and fail to recognize the complexity of the financial payment systems underlying their consumer relationships and purchases. This is particularly true with respect to entities with whom financial and retail organizations outsource operations, such as data brokers like ChoicePoint.[125] A definition of the problem as a lack of public awareness includes the following considerations: the ability, or lack thereof, of individuals to make wise personal decisions with respect to their dealings

---

121. *See* Andrew Conry-Murray, *PCI and the Circle of Blame*, INFO. WK., Feb. 25, 2008, at 30 (explaining how compliance with certain industry security standards helps a company appear protected without actually improving the security of their data stores).

122. *See* Paul M. Schwartz & Edward J. Janger, *Notification of Data Security Breaches*, 105 MICH. L. REV. 913, 925-31 (2007) (identifying and explaining three forces pressuring companies: regulatory, economic, and reputational).

123. *See* ROBERT O'HARROW JR., NO PLACE TO HIDE 44-45 (2006) (describing the increase in information acquisition and corresponding lack of individuals' awareness using Acxiom as an example); Dennis Hoffman & Ken Tyminski, *From Financial Services CISO to Chief Information Management Office: Tackling 360 Degrees of Enterprise Protection*, WALL ST. & TECH., April 26, 2007 (showing the "gap" in knowledge of financial institutions); Melanie Rodier, *Locking the Back Door*, WALL ST. & TECH., Nov. 1, 2007, at 26 (giving examples of "major security hole[s]" companies are overlooking).

124. Stacey L. Schreft, *Risks of Identity Theft: Can the Market Protect the Payment System?*, 92 ECON. REV. FED. RES. BANK KAN. CITY 5 (2007).

125. *See generally* Chris Jay Hoofnagle, *Big Brother's Little Helpers: How ChoicePoint and Other Commercial Data Brokers Collect and Package Your Data for Law Enforcement*, 29 N.C. J. INT'L L. & COM. REG. 595 (2004) (describing the relationship, or lack thereof between the "individual" and the "organization" in relation to information privacy).

with other individuals because of lack of knowledge, and the competence of the public as a whole to understand the dynamics and contours of the information social and economic environment in which they operate on a daily basis. The goal is to enable individuals, singularly and collectively, to make more informed and more socially desirable decisions.

Notification of security breaches is a solution that can address each of these policy problems. The question of the effectiveness of security breach notices as a solution is next analyzed in terms of the likelihood of such notices achieving these different policy goals.

*3. Effectiveness of Notices*

a) Critics and Supporters

Some critics have argued that the effectiveness of notices is over-stated and that individuals will ignore the notices, especially if notices are sent for relatively minor breaches or sent too often. As the president of the Information Technology Association of America, Harris Miller, noted, "it's like crying wolf . . . . You're actually undermining the companies' ability to get customers to pay attention when there's a real data breach."[126] Pointless notices can also impose unnecessary costs on consumers if they cancel credit cards, place fraud alerts on credit files, or obtain new driver's license numbers.[127] Other critics have pointed out that "[n]otification letters supply only incomplete, discontinuous, and non-comparative information about data security," sending consumers a "fuzzy signal about future behavior and the likelihood of additional data security breaches."[128] Still others emphasize, as Fred Cate does, that notice "is always a *response* to an event after it has occurred, rather than the *prevention* of that event."[129] In general, industry is opposed to broad notification requirements, seeing them as "expensive, embarrassing, confusing to consumers and often unnecessary."[130] Instead, industry prefers notice in instances where there is a significant chance of harm to the individual with industry being the main determinant of when that might be.

---

126. Patton, *supra* note 27.

127. *Data Breaches and Identity Theft: Hearing Before the S. Comm. on Commerce, Science and Transportation* 109th Cong. (2005) (statement of Deborah Platt Majoras, Chairman, FTC), *available at* http://www.ftc.gov/os/2005/06/050616databreaches.pdf.

128. Schwartz & Janger, *supra* note 122, at 947.

129. Fred H. Cate, *Information Security Breaches: Looking Back and Thinking Ahead*, Centre Info. Pol'y Leadership Hunton & Williams LLP, at 6 (2008) (emphasis in original), http://www.hunton.com/files/tbl_s47Details/FileUpload265/2308/Information_Security_Breaches_Cate.pdf.

130. Jacob Freedman, *Industry Seeks One Law on Data Breach Alerts*, 64 CONG. Q. WKLY. REP. 314, 314 (2006).

Conversely, supporters of notice requirements see enormous value in providing an incentive for an organization to protect sensitive information and encouraging organizations to audit their own security measures. Notice is a mechanism not only for informing individuals who are the subject of a data breach, but also the press and other industry players. Indeed, one could argue that the legislative interest in security breach notification, at both the state and federal level, would not have occurred without the notices that resulted from the California law. Moreover as Representative Janice D. Schakowsky (D-Ill.) pointed out, concern about over-noticing is "disingenuous" as "[t]he right response to over-notification is not to restrict information and to keep consumers and Congress in the dark. If we want to stop over-notification, then corporations need to clean up their act so consumers' personal information is not compromised in the first place."[131]

b) Effectiveness in meeting policy goals

As introduced above, security breach notifications are offered as a solution to a policy problem that has been defined in at least three different ways. The effectiveness of notices is next considered with respect to each of these problems—reducing identity theft, improving organizational data security, increasing public awareness—and the corresponding policy goal.

First, consider notification as a way of reducing identity theft. There is some question about the extent to which security breaches cause instances of identity theft.[132] A survey conducted by Javelin in 2007 revealed that respondents attributed very few reported incidents of identity theft to security breaches.[133] Similarly, the GAO found that based on available data and interviews with law enforcement and industry representatives, most security breaches did not result in detected incidents of identity theft, particularly in the unauthorized creation of new accounts.[134] In only three of the twenty-four largest security breaches between January, 2000 and June, 2005 did the GAO find evidence of misuse of personal information and in only one breach was there evidence of identity theft.[135] Romanosky, Telang, and Ac-

131. Krim, *supra* note 93, at D04.

132. *See* Brendan St. Amant, *Recent Development: The Misplaced Role of Identity Theft in Triggering Public Notice of Database Breaches*, 44 HARV. J. ON LEGIS. 505, 520-22 (2007) (discussing the difficulty in measuring the risk of identity theft).

133. CATE, *supra* note 129, at 8 (citing JAVELIN STRATEGY AND RESEARCH, IDENTITY FRAUD SURVEY REPORT (2007)).

134. U.S. GOV'T ACCOUNTABILITY OFFICE, PERSONAL INFORMATION: DATA BREACHES ARE FREQUENT, BUT EVIDENCE OF RESULTING IDENTITY THEFT IS LIMITED; HOWEVER, THE FULL EXTENT IS UNKNOWN, GAO-07-737 (2007), *available at* http://www.gao.gov/new.items/d07737.pdf.

135. *Id.*

quisti analyzed the impact of data breach disclosure laws on identity theft for the years 2002 to 2006 and found that the laws had no statistically significant effect on reducing identity theft.[136]

If one finds this evidence convincing, then security breach notification is unlikely to be directly effective in reducing identity theft. There may, however, be indirect positive effects on the reduction of identity theft, as individuals who receive security breach notifications will generally be more cognizant of ways to protect their information.[137] Increased information about security breaches may raise individuals' awareness of the risks of inadvertent disclosure of their information and in the uncertainties about information handling practices—and this may change their individual behavior, reducing their risk of identity theft.[138] Anecdotal evidence and public opinion surveys tend to support the indirect positive effects from security breach notifications and the concomitant media and public attention.[139] A 2006 survey conducted for the Chief Marketing Officers Council concluded that consumers have become more concerned about security and that "[t]hese concerns seem to be driven by personal experiences with security problems, which in turn have been made more prevalent by the personal notification of security breaches."[140]

Second, security breach notification is viewed as a means of improving organizational data security practices. Although notice is not effective in preventing the security breach that triggered the notice, it can act as a deterrent against future events by that specific organization and other similarly situated organizations. Security breach notification may be effective in encouraging a "culture change" within organizations so that data security becomes more of

136. Sasha Romanosky et al., *Do Data Breach Disclosure Laws Reduce Identity Theft?*, (Seventh Workshop on the Economics of Information Security, Working Paper, 2008), at 13-14, *available at* http://weis2008.econinfosec.org/papers/Romanosky.pdf (noting the possibility of reporting bias for identity theft and the possibility that there are "other means by which this law could (and should) be evaluated").

137. Olive Huang et al., *Security Breach Notification Laws: Views from Chief Security Officers*, SAMUELSON L., TECH. & PUB. POL'Y CLINIC, Dec. 2007, at 24, *available at* http://groups.ischool.berkeley.edu/samuelsonclinic/files/cso_study.pdf.

138. *Id.*

139. *See* PRIVACY RIGHTS CLEARINGHOUSE, HOW MANY IDENTITY THEFT VICTIMS ARE THERE? WHAT IS THE IMPACT ON VICTIMS? (2007), http://www.privacyrights.org/ar/idtheftsurveys.htm#Jav2007 (summarizing recent surveys to show identity theft trends); *see also* FEDERAL DEPOSIT INSURANCE CORPORATION, PUTTING AN END TO ACCOUNT-HIJACKING IDENTITY THEFT (2004), http://www.fdic.gov/consumers/consumer/idtheftstudy/identity_theft.pdf.

140. Huang et al., *supra* note 137, at 23 (citing CHIEF MARKETING OFFICER COUNCIL, SECURE THE TRUST OF YOUR BRAND: ASSESSING THE SECURITY MINDSET OF CONSUMERS 8 (2006)).

a priority and more integral to business practices. As security breach notification entails a number of real and potentially significant costs to an organization, including "damage to brand reputation, loss of current [or] future customers, liability under state laws, and [] possible lawsuits,"[141] organizations should seek to avoid or lower these costs by decreasing their number of security breaches. A Ponemon Institute survey in 2007 found that forty percent of retail customers would consider terminating a relationship with a company that experiences a data breach, although only nineteen percent actually did so.[142] Similarly, a 2007 survey of 1200 debit card customers by Javelin Strategy and Research found that three out of four would stop shopping at a store where a data breach occurred and more than three-quarters said they would shop at stores that were security leaders.[143] The reputational harm, or "public shaming,"[144] alters the environment in which organizations find themselves operating. The harm may provide opportunities for those organizations with more effective data security policies and practices to use them competitively.

Third, security breach notifications are seen as a technique for increasing public awareness about the ways in which personally identifiable information is collected, exchanged, and retained. There is evidence that notices are effective in this respect. For example, the simple fact that so many states followed the example of California in passing such laws after the ChoicePoint breach (and the state-law mandated consumer notification of the breach) lends support to the effectiveness of notification in increasing public awareness.[145] Notices are also effective in alerting the media and the advocacy community. In a study conducted by the Samuelson Law, Technology and Public Policy Clinic, "organizations noted concerns that a public notification of a breach would damage their organizations' reputation and the trust behind their name."[146] In their interviews with chief security officers, they also found that,

---

141. Patrick R. Mueller, *How to Survive Data Breach Laws*, NETWORK COMPUTING, June 8, 2006, at 8.

142. Patrick R. Mueller, *Changing Landscape of Data-Breach Notification*, NETWORK COMPUTING, May 14, 2007, at 18.

143. Larry Greenemeier, *Data Theft, Pushback and the TJX Effect – Details of the Largest Customer Data Heist in U.S. History are Beginning to Emerge*, INFO. WK., Aug. 13, 2007, at 36.

144. Zeller, *The Scramble to Protect Personal Data*, *supra* note 7, at C1. *See also* BRUCE SCHNEIER, SECRETS AND LIES: DIGITAL SECURITY IN A NETWORKED WORLD 37-38 (Paperback ed. 2004) (describing the reputational dangers to companies of security attacks).

145. *See*, *e.g.*, Zeller, *Another Data Broker Reports a Breach*, *supra* note 7, at C1; Zeller, *Breach Points Up Flaws in Privacy Laws*, *supra* note 6, at C1; Zeller, *The Scramble to Protect Personal Data*, *supra* note 7, at C1 (describing the impacts of consumer notifications following security breaches by data brokers). *See generally* Nakashima, *supra* note 19 (describing the state of security breach notification laws in early 2007 in the context of the security breach at T.J. Maxx and Marshalls retail stores).

146. Huang et al., *supra* note 137, at 15.

with the passage of security breach notification laws, organizations were being advised to invest in encryption.[147] Without notices, less information about breaches would be available; therefore they are effective in reducing the information gathering costs for the public. In this way security breach notifications operate in a similar fashion to notices in the environmental and consumer areas.[148] Indeed, the Samuelson study found that as a result of security breach notification letters and media coverage, security and information privacy was a "hot topic in consumer protection discussions."[149]

c) Lessons from other attempts at "targeted transparency"

The response to the shortcomings that have been identified with security breach notifications need not be to dismiss notification letters as ineffective, but rather to strive to identify ways in which they can be made more effective. In providing notices to individuals, it is critical that the notice be worded in such a way that the individual is not overloaded with irrelevant information, and that the form and content of the notice is understandable. In terms of fashioning effective notices, the research and findings of Fung et al. are particularly instructive, noting that interest in transparency policies is increasing because the more conventional forms of government intervention are not well suited to policy areas that involve "risks and performance flaws" and characterized by wide differences in consumers' preferences, such as consumer decisions about, for example, the relationship between saturated fats and heart disease.[150] Rather than direct government intervention, such as taxing or banning certain products, requiring notification to consumers is seen as an effective role for government.[151] They also point out that the Internet has generated more interest in transparency as "the Internet provides new ways to customize and share information about the risks companies create and the quality of the products and services they provide."[152]

---

147. *Id.* at 17-18.

148. *See*, *e.g.*, Michael S. Baram, *The Right to Know and the Duty to Disclose Hazard Information*, 74 AM. J. PUB. HEALTH 385, 385 (1984) ("[T]he Occupational Safety and Health Administration['s] . . . rule imposes on these employers the duty to disclose such privately held information."); Judith A. Garretson, *Effects of Nutrition Facts Panel Values, Nutrition Claims, and Health Claims on Consumer Attitudes, Perceptions of Disease-Related Risks, and Trust*, 19 J. PUB. POL'Y & MARKETING 213, 223 (2000) (discussing the Nutrition Labeling and Education Act's objective in mandating nutrition labels to "provide information that consumers can use effectively to make more healthful food judgments and choices").

149. Huang et al., *supra* note 137, at 23.

150. FUNG ET AL., *supra* note 58, at 14.

151. *Id.*

152. *Id.* at 14-15.

Through a detailed analysis of fifteen targeted transparency systems, Fung et al. sought to explain what made the difference between a successful policy and an unsuccessful one.[153] They point out, for example, that effective policies provide facts in ways that people want in times, places, and ways that enable them to act.[154] Traditional privacy notices are often crafted with detailed information regarding detailed aspects of information handling which individuals do not see as relevant.[155] Fung et al. also note that effective policies increase knowledge that informs choice rather then providing information that is not directly related to an action.[156] And they argue that there need to be sanctions for non-reporting and misreporting.[157]

*4. Scope of Policy*

The fourth substantive policy issue regarding proposed federal security breach notification legislation involves the larger context in which such notifications would operate. There are several controversial questions involved here which this Article will only briefly touch. Each, however, has been, and is likely to continue to be controversial.[158] The most controversial question is what standard should be used to "trigger" a notification, including whether the seriousness of the breach should be "reasonably likely" or "reasonably possible," and whether the standard of risk should be that the information could be "misused" or that the breach poses a "significant risk of identity theft" or a "material risk of harm." Predictably, consumer groups support a lower standard, such as "reasonably likely" while companies favor a higher standard, such as "substantial" or "significant."[159] A related question to when notifications would be required involves whether the breach has to affect a certain number of individuals. Finally, related to the issue of triggers for notification is the question of whether encrypted data should be exempted. The

153. *Id.* at 12-13, 183-208 (including analysis of transparency systems spanning a wide range of areas such as terrorism, environmental hazards, personal safety, finance and lending, and food and beverage safety).

154. *Id.* at 11; *accord* David Gibson, Carla Hall & Sylvia Harris, *Healthy Credit*, N.Y. TIMES, May 24, 2009, at WK9 (comparing new credit card policies to food packaging nutrition labels to be "written with the cardholder in mind").

155. George R. Milne et al., *A Longitudinal Assessment of Online Privacy Notice Readability*, 25 J. PUB. POL'Y & MARKETING 238, 245-46 (2006).

156. *See* FUNG ET AL., *supra* note 58, at 177.

157. *Id.* at 179.

158. *See generally* DATA SECURITY, *supra* note 31 (reviewing and summarizing these issues and relevant congressional bills).

159. Stern, *supra* note 89, at 1032.

possibility of an exemption of this kind has sparked debate about the appropriate level of encryption that should be required.[160]

Congressional and public deliberations regarding security breach notifications have also involved questions about several related issues that are often included in policy proposals. Prominent among these are restrictions on use of Social Security Numbers (SSN), which are widely recognized as critical to information security. More controls on, and less use of, SSNs will reduce the dangers to data subjects if their data is compromised. Several congressional bills dealing with security breach notifications have also included restrictions on SSNs, such as eliminating their use as an identifier or authenticator, which are resisted by some organizations because they would impose costs of reconfiguring systems.[161] Another controversial issue has involved whether consumers can freeze their consumer credit reports after a security breach, enabling consumers to block unauthorized third parties from accessing their credit reports. Consumer groups argue that such credit freezes protect consumers from someone fraudulently opening credit in the name of someone whose data have been breached.[162] Business groups argue that such freezes are not necessary as consumers can request fraud alerts under the Fair Credit Reporting Act.[163]

In general, notices are not a "stand-alone" solution, but rather they provide the centerpiece of a more comprehensive policy response that also includes some public reporting, often to a government entity charged with overseeing the policy, and civil fines and criminal penalties if an organization knowingly covers up a breach. For example the Florida security breach notification law fines companies $1,000 a day for each day they fail to disclose a

160. *See Hearing*, *supra* note 117, at 113-14 (citing Bill Watkins, Chief Information Officer for Seagate Technologies in a March 21, 2007 statement recommending that legislation should include a "safe harbor" from regulation if an organization used "hard disc drive-based full encryption" on stored information). In the proposed regulations for implementing the HITECH Act, the FTC and HHS would exempt encrypted stored data from notification requirements if they meet the NIST standards set forth in Publication 800-111 *Guide to Storage Encryption Technologies for End User* and data in transmission if they comply with the requirements of Federal Information Processing Standards (FIPS) 140-2, which include the standards set forth in NIST Special Publications 800-52, *Guidelines for the Selection and Use of Transport Layer Security (TLS) Implementations;* 800-77, *Guide to IPsec VPNs*; or 800-113, *Guide to SSL VPNs, or other guidance* validated by FIPS 140-2. Thomas J. Smedinghoff & Shannon M. Travis, *HHS and FTC Issue Proposed Regulations on Breach Notification Requirements for Health Records*, WILDMAN HAROLD CLIENT BULLETIN, May 20, 2009, http://www.wildman.com/bulletin/05202009.

161. *See*, *e.g.*, Identity Theft Protection Act, S. 1408, 109th Cong. (2005); Personal Data Privacy and Security Act, S. 1332, 109th Cong. (2005).

162. Stern, *supra* note 89, at 1033.

163. *Id.*

breach, with a monthly fine of $50,000 after thirty days.[164] A Montana law punishes failures to disclose with fines of $10,000 per violation and possible criminal charges.[165] Several congressional bills incorporate similar civil and criminal penalties.[166] Additionally the public reporting to an oversight entity is an important component of most state laws, which generally require reporting to the state attorney general.[167] In congressional bills, reporting is often to the relevant regulatory commission or to the FTC,[168] but the efficacy of such oversight depends on whether these organizations have the personnel and budget to shoulder these new responsibilities. Providing new oversight responsibilities without adequate resources is not likely to be effective. In this respect, Schwartz and Janger propose the establishment of a Coordinated Response Agent (CRA) which would oversee the notification process.[169]

## V. CONCLUSION: LIKELIHOOD OF PASSAGE

By mid-2007, there was some sense that the policy window that opened for passage of security breach notification laws had already closed without policy action.[170] As states continued to fill the void left by federal inaction and passed more state laws, it appeared to some that federal action was unnecessary and potentially dangerous for consumers.[171] Evan Hendricks, editor of *Privacy Times*, noted that "[w]ith so many conflicting agendas from the financial industry, data brokers and security companies, there is the danger any bill could be watered down."[172] The likelihood that security breach notification bills will be watered down is very real and very much to be expected given that they fit the classic pattern of regulatory policies, imposing costs on a smaller, well-defined group and providing benefits for a largely dispersed (and often inattentive) group.[173] In order for such policies to pass, it is important that there are groups advocating in support of the policies. Moreover,

164. FLA. STAT. § 817.5681(1)(b) (2009).

165. MONT. CODE ANN. § 30-14-142 (2007).

166. *E.g.*, Financial Privacy Breach Notification Act, S. 1216, 109th Cong. (2005) (authorizing a customer injured by a violation to institute a civil action to recover damages).

167. *E.g.*, N.H. REV. STAT. ANN. § 359-C:20(I)(b) (2009).

168. *E.g.*, Data Accountability and Trust Act (DATA), H.R. 4127, 109th Cong. (2005); Identity Theft Protection Act, S. 1408, 109th Cong. (2005).

169. Schwartz & Janger, *supra* note 122, at 960.

170. Jon Swartz, *Lawmakers Get Less Combative on Data-Breach Bills: Change from Previous Years*, U.S.A. TODAY, March 1, 2007, at 5B.

171. *Id.*

172. *Id.*

173. *See* RANDAL B. RIPLEY & GRACE A. FRANKLIN, BUREAUCRACY AND POLICY IMPLEMENTATION (1982); JAMES Q. WILSON, POLITICAL ORGANIZATIONS (1974); Lowi, *supra* note 9.

such policies are more likely to pass when there has been a crisis or event that brings public attention to the harms that have occurred and that would be redressed by the policies under discussion.

By mid-2009, the odds for passage of security breach notification laws may well have increased.[174] Not only have interest groups continued to advocate for passage, but incidents of security breaches continue to occur and to receive media attention. Perhaps more importantly, the current political climate and financial crisis—with a policy response that emphasizes transparency and accountability, as well as disparagement for those who are causing "moral hazards"—is more conducive to the passage of some legislation.

Recent congressional actions on the HITECH Act and the Credit Card Act of 2009, which requires a forty-five day notice of changes in terms for credit cards,[175] as well as House subcommittee action on the Data Accountability and Trust Act of 2009 are evidence of a more receptive congressional response to legislation that places restrictions on financial institutions that have benefited at significant cost to consumers and the economy as a whole. If security breach notification legislation is viewed by members of Congress through this new perceptual lens, then the likelihood that the previous barriers to passage will be overcome is increased.

174. *See* Neuburger & Krauss, *supra* note 43 (describing the relevant HITECH Act provisions for "protected health information" passed this year, indicating passage of federal security breach notification laws).

175. Phil Mattingly, *Credit Card Restrictions Enacted*, CONG. Q. WKLY. REP., May 25, 2009, at 1214.