

COMMENT

DATABASE SECURITY BREACH NOTIFICATION STATUTES: DOES PLACING THE RESPONSIBILITY ON THE TRUE VICTIM INCREASE DATA SECURITY?*

TABLE OF CONTENTS

- I. INTRODUCTION 1598
- II. IDENTITY THEFT AND DATABASE SECURITY BREACH:
 - A PROBLEM DEFINED..... 1600
 - A. *What Is Identity Theft?* 1600
 - B. *Types of Identity Theft* 1602
 - C. *Database Security Breach and Identity Theft* 1603
 - 1. *Security Breach*..... 1604
 - 2. *The Connection Between Security Breach and Identity Theft* 1604
- III. PRIVACY VS. DATA CONTROL..... 1605
 - A. *Distinguishing Privacy from Data Protection* 1606
 - B. *Privacy Rights and Freedom of Speech—A Balancing Act* 1609
- IV. CURRENT DATA PROTECTION LEGISLATION 1612
 - A. *Federal Legislation Requiring the Implementation of Privacy and Security Policies*..... 1613
 - 1. *Health Insurance Portability and Accountability Act*..... 1613
 - 2. *Children’s Online Privacy Protection Act* 1615

* This paper received the Locke Liddell & Sapp, LLP Award for the outstanding paper in the area of banking and corporate law. The Author would like to thank Raymond T. Nimmer, professor and Dean of the University of Houston Law Center, for his support and invaluable guidance in the development of this Comment.

But the secret is out. News reports of security breaches exposing consumer data to cyber criminals are sounding the horn—identity theft in this country is on the rise. In June 2005, a hacker accessed over 40 million MasterCard International customers' credit card accounts.⁵ That same month, the FDIC had to admit that 6,000 of its employees' personal data might have been stolen.⁶ And in February 2005, ChoicePoint, Inc. announced that identity fraudsters gained access to 145,000 people's personal identification data by setting up fifty phony companies.⁷ These types of events have prompted legislators to enact laws that deal with the way personal information is handled.⁸

For example, California legislators took an innovative approach when they passed the Database Security Breach Notification Act ("Notification Act").⁹ The law places responsibility on data holders to keep customer information secure, requiring the data holders to disclose any actual or potential security breaches, which allows consumers to take curative measures.¹⁰ This Comment argues that security breach notification statutes like California's are effective ways to deal with identity theft because the costs involved with public disclosures of security breaches will induce companies to implement more responsible security measures.

Part II of this Comment defines identity theft and explores its connection to database security breach. Part III discusses the difference between traditional privacy concerns and modern data control issues to provide a better understanding of the policy considerations evident in identity theft legislation. Part IV looks at the current major data protection laws in the United States,

5. See Michael Gormley, *ID Theft Law Requires Disclosing Security Breaches*, BUFFALO NEWS, Aug. 14, 2005, at A11.

6. Pizzo, *supra* note 4, at 6.

7. Matt Hines, *ChoicePoint Data Theft Widens to 145,000 People*, CNET NEWS.COM, Feb. 18, 2005, http://news.com.com/ChoicePoint+data+theft+widens+to+145,000+people/2100-1029_3-5582144.html. The fraudulently obtained information included names, addresses, and social security numbers. *Id.*

8. See Grant Gross, *Senators Rip into ChoicePoint, Bank of America*, INFOWORLD, Mar. 10, 2005, http://www.infoworld.com/infoworld/article/05/03/10/HNsenatorsripchoice_1.html (describing planned and proposed legislation regulating data collectors' use and protection of private information); Raymond T. Nimmer, *Privacy, Data Protection and Security Balance* (Sept. 6, 2005), <http://www.ipinfoblog.com/archives/privacy-data-protection-and-security-31-privacy-data-protection-and-security-balance.html> (stating that the multitude of publicly disclosed security breaches have galvanized a push for data security legislation).

9. S.B. 1386, 2002 Leg., Reg. Sess. (Cal. 2002) (codified as amended at CAL. CIV. CODE §§ 1798.29, .82 (West Supp. 2006)).

10. *Id.*

paying particular attention to database breach notification statutes. Part V analyzes the costs and benefits of the notification duty imposed on businesses by security breach notification laws, arguing that such a duty produces adequate protection against identity fraud to justify the costs involved. Finally, Part VI concludes that breach notification statutes are an effective instrument to fight identity theft, suggesting that a federal uniform law is a sound approach to implement mandatory security breach notifications nationwide.

II. IDENTITY THEFT AND DATABASE SECURITY BREACH: A PROBLEM DEFINED

To appreciate the nature of the problem caused by security breach, it is imperative to understand how identity theft occurs and how victims of the crime are affected by it. Equally important is an understanding of the connection between identity theft and database security breach, and the large-scale ramifications of that combination.

A. *What Is Identity Theft?*

Identity theft is becoming “the crime of the new millennium.”¹¹ The U.S. General Accounting Office defines it as “stealing’ another person’s personal identifying information . . . and then using the information to fraudulently establish credit, run up debt, or take over existing financial accounts.”¹² An identity thief gains access to an individual’s name, social security number,¹³ date of birth, and other important information either to impersonate the individual and obtain goods and services in the victim’s name,¹⁴ or to obtain independent employment and government benefits.¹⁵ Identity

11. Sean B. Hoar, *Identity Theft: The Crime of the New Millennium*, 80 OR. L. REV. 1423, 1423 (2001).

12. U.S. GEN. ACCOUNTING OFFICE, IDENTITY THEFT: GREATER AWARENESS AND USE OF EXISTING DATA ARE NEEDED 1 (2002), available at <http://www.gao.gov/new.items/d02766.pdf>.

13. Social security numbers are pivotal to identification authentication because data concerning tax, credit, school, and medical records are keyed to one’s social security number, making it valuable to identity thieves. See EPIC Social Security Number (SSN) Privacy Page, Social Security Numbers, <http://www.epic.org/privacy/ssn/> (last visited Jan. 10, 2007).

14. Mark E. Budnitz, *Privacy Protection for Consumer Transactions in Electronic Commerce: Why Self-Regulation Is Inadequate*, 49 S.C. L. REV. 847, 858 (1998).

15. See Timothy H. Skinner, *California’s Database Breach Notification Security Act: The First State Breach Notification Law Is Not Yet a Suitable Template for National Identity Theft Legislation*, 10 RICH. J.L. & TECH. 1, ¶ 10 (2003), <http://law.richmond.edu/>

crooks use their victims' personal information to access or create accounts with various merchants or service providers, such as utility companies, banks, schools, and government organizations.¹⁶ As a result, identity-theft victims are left with false records and unpaid debt, among other problems.¹⁷

Aside from financial loss, victims also experience angst, a diminished sense of privacy and security, and difficulty "obtaining loans, mortgages, security clearances, promotions and even gaining employment."¹⁸ Moreover, once the crime is discovered, the problem is not easily solved. Unlike stolen goods—where the value of the property represents a one-time loss—the harm caused by a stolen identity is ongoing.¹⁹ Even after the affected individual has cleared her name and credit history, the risk of further harm will linger as long as the thief remains at large and in possession of the victim's personal identification data.²⁰

Identity theft is costing Americans billions of dollars a year.²¹ In 2002, identity thieves acquired goods and services costing business and financial institutions an average of \$10,200 per victim, amounting to \$47 billion in total loss, and costing individual victims \$500 on average.²²

The subtle nature of the crime compounds the problem. The average time to discover identity theft is fourteen months,²³ and the process of recovery is even longer.²⁴ The amount of time and money spent dealing with the problem also depends on the type

jolt/v10i1/article1.pdf (describing possible uses by identity thieves of stolen personal information).

16. See Daniel J. Solove, *Identity Theft, Privacy, and the Architecture of Vulnerability*, 54 HASTINGS L.J. 1227, 1245 (2003).

17. *Id.* at 1245–46.

18. Martha A. Sabol, *The Identity Theft and Assumption Deterrence Act of 1998: Do Individual Victims Finally Get Their Day in Court?*, 11 LOY. CONSUMER L. REV. 165, 167 (1999).

19. Solove, *supra* note 16, at 1245–46.

20. *Id.*

21. Ellen McCarthy, *PayAgent Aims to Curtail Identity Theft Online*, WASH. POST, Sept. 8, 2003, at E5 (noting the Federal Trade Commission's (FTC) estimate that identity theft cost individuals and businesses \$5 billion and \$48 billion respectively in 2002). For instance, from mid-2002 to mid-2003, approximately seven million people fell victim to identity theft. Identity Theft Res. Ctr., *Facts and Statistics*, <http://idtheftcenter.org/facts.shtml> (last visited Jan. 10, 2007). Each victim spent an average of 600 hours and \$1,400 dealing with the aftermath of the crime. *Id.*

22. SYNOVATE, FEDERAL TRADE COMMISSION—IDENTITY THEFT SURVEY REPORT 6 (2003) [hereinafter 2003 FTC REPORT], available at http://www.consumer.gov/idtheft/pdf/synovate_report.pdf.

23. Skinner, *supra* note 15, ¶ 13.

24. See Hoar, *supra* note 11, at 1425–26 (stating that, once discovered, it may take a victim "months or years" to recover from identity theft).

of identity theft involved.²⁵ All of these factors help to create a crime difficult to recognize or remedy.

B. *Types of Identity Theft*

Crimes of identity fraud can be classified into several broad categories: (1) fraudulent authentication or one-time identity theft, (2) financial institution fraud, (3) credit card fraud, (4) fraudulent loans, (5) communications and utilities fraud, and (6) other miscellaneous frauds.²⁶ Identity thieves employ various methods to obtain personal information. Some fraudsters resort to “basic street theft,” while others develop complex schemes seeking to compromise computer databases or bribe employees with access to customer records.²⁷

Basic street theft is the traditional and most common method of identity theft.²⁸ A fraudster may obtain identification data by grabbing a lost or stolen wallet that contains credit cards, identification documents, checkbooks, and social security cards.²⁹ Alternatively, a street theft may occur by digging through one’s garbage to steal mail containing personal information.³⁰ The Internet, fast becoming the primary venue for identity crooks, is a more modern vehicle for identity theft.³¹ Computerized databases that contain personal identification information are vulnerable to hackers who can access them via the Internet.³²

25. *Prepared Statement of the Federal Trade Commission: Hearing to Examine Federal Legislative Solutions to Data Breach and Identity Theft Before the S. Comm. on Commerce, Science, and Transportation*, 108th Cong. 3–4 (2005) [hereinafter *FTC Statement*] (statement of Deborah Platt Majoras, Chairman, Federal Trade Commission) (citing 2003 FTC REPORT, *supra* note 22), available at <http://commerce.senate.gov/pdf/ftc.pdf>.

26. Holly K. Towle, *Identity Theft: Myths, Methods, and New Law*, 30 RUTGERS COMPUTER & TECH. L.J. 237, 242 (2004).

27. *Id.* at 241 (quoting S. REP. NO. 105-274, at 6 (1998), available at http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=105_cong_reports&docid=f:sr274.105.pdf).

28. *See id.* at 238–39 (referring to a FTC survey reporting that basic street theft is the most common method for obtaining stolen information).

29. *Id.*

30. *Id.*

31. *See id.* at 248 (“The Internet has the potential to become a primary resource for fraudsters to steal identities.” (quoting NAT’L AUTOMATED CLEARING HOUSE ASS’N INTERNET COUNCIL, INTERNET PAYMENTS FRAUD: A PRIMER FOR MERCHANTS AND FINANCIAL INSTITUTIONS 15 (2003), available at <http://internetcouncil.nacha.org/docs/Fraud%20Paper%20Final%20Jan%20%2703.pdf>)).

32. *Id.* (quoting NAT’L AUTOMATED CLEARING HOUSE ASS’N INTERNET COUNCIL, *supra* note 31, at 15).

C. Database Security Breach and Identity Theft

Computerized databases containing personal information on large numbers of people are a perfect one-stop shopping place for identity thieves. Any one database intrusion exposes numerous individuals to identity theft.³³ Although database security breach has not become the prevalent method for identity theft,³⁴ it has the potential for becoming a crime of grand proportions. Not surprisingly, the recent avalanche of public disclosures of security breaches resulted in a push for legislative solutions to the problem.³⁵

Database software and services represent a multi-billion dollar industry.³⁶ Computer technology has revolutionized data collection, allowing it to become a lucrative business both on- and offline.³⁷ Data collectors use the information for various reasons, including research documentation and tracking consumer consumption for marketing purposes.³⁸ Financial, governmental, educational, and other business institutions also compile huge databases containing individuals' personal information.³⁹ And with the rise of e-commerce, more and more databases containing such information risk penetration by cyber criminals.⁴⁰

33. Businesses and governmental agencies keep various types of personal information in one database, allowing a thief to access several pieces of one's personal data. See, e.g., Robert Lemos, *Data Thieves Nab 55,000 Student Records*, CNET NEWS.COM, Mar. 6, 2003, <http://news.com.com/2100-1002-991413.html> (noting that the University of Texas at Austin's database, containing thousands of students' names, social security numbers, addresses, and e-mail accounts, was successfully hacked and more than fifty thousand records were compromised).

34. See 2003 FTC REPORT, *supra* note 22, at 9, 30 (identifying loss or theft of wallets and mail as the primary way identity thieves obtain information), *cited in* Towle, *supra* note 26, at 238–39.

35. See *infra* Part IV (discussing major current data protection legislation in the United States).

36. See Laflamme, *supra* note 2, at S6 (reporting that in 2001 database software services were estimated at \$9 billion).

37. *Id.*

38. See Stefanie Olsen, *FTC: All Eyes on Consumer Privacy*, CNET NEWS.COM, June 10, 2004, http://news.com.com/FTC:+All+eyes+on+consumer+privacy/2100-1024_3-5230750.html (discussing companies' uses of technology to monitor consumers' online activities and purchases and companies' uses of customer profiling for the purposes of targeted advertising).

39. *Cf.* Lemos, *supra* note 33 (reporting a security breach in the University of Texas at Austin's database containing over 55,000 students' identifiable information); *Root of Massive Credit Card Theft Found*, CNN.COM, Feb. 20, 2003, <http://www.cnn.com/2003/TECH/internet/02/20/credit.hack.ap/index.html> (announcing that eight million credit card numbers were stolen from "a company that handles transactions for catalog companies and other direct marketers").

40. *Cf.* Laflamme, *supra* note 2, at S6 (describing how consumers using the Internet provide personal information to websites that track and collect such data).

1. *Security Breach.* A security breach can be defined as “a successful attack on a computer system’s security controls in order to penetrate the system to acquire or corrupt information on the system, thus disrupting the confidentiality, integrity, or availability of information on the system.”⁴¹ A system can be breached externally or internally.⁴² An external breach is orchestrated by a hacker who breaks into the system to access information contained in the database.⁴³ An internal job is executed by an employee or system administrator with rightful access to the data.⁴⁴

Whether done externally or internally, computer system invasions occur at an alarmingly frequent rate. The Computer Security Institute reported that in 2003, 56% of respondents surveyed experienced security breaches—costing those organizations in excess of \$201 million.⁴⁵

2. *The Connection Between Security Breach and Identity Theft.* The aforementioned intrusions expose thousands of individuals to the risk of identity theft.⁴⁶ Thus, a responsive social policy dictates that companies compiling and storing personal identification data sought by identity fraudsters should protect this data from unauthorized access. Sadly, data-collecting organizations that handle millions of people’s personal information do not have a strong culture of data security.⁴⁷

The number of database security breaches has grown, with news sources reporting incidents of security breaches and stolen personal information on a nearly constant basis.⁴⁸ The public

41. Skinner, *supra* note 15, ¶ 5.

42. *Id.* ¶ 6.

43. *Id.*

44. *Id.*

45. COMPUTER SEC. INST., 2003 CSI/FBI COMPUTER CRIME AND SECURITY SURVEY 3 (2003) [hereinafter SECURITY SURVEY], available at http://i.cmpnet.com/gocsi/db_area/pdfs/fbi/FBI2003.pdf.

46. See *supra* notes 11–17 and accompanying text (defining identity theft and explaining how fraudsters steal an individual’s identity). Many companies are not even aware of security breach occurrences, yet they are expected to actively protect their customers’ identities. See SECURITY SURVEY, *supra* note 45, at 8 (reporting that at least 15% of the respondents were unaware of whether there was any unauthorized use of their systems).

47. Skinner, *supra* note 15, ¶ 7.

48. Recent examples paint an alarming picture. ChoicePoint announced a security breach that resulted in 145,000 false accounts established by identity thieves. Privacy Rights Clearinghouse, *A Chronology of Data Breaches*, Apr. 20, 2005, <http://www.privacyrights.org/ar/ChronDataBreaches.htm>. Bank of America’s lost backup tape exposed 1.2 million people’s personal information. *Id.* DSW/Retail Ventures reported that hackers accessed 100,000 accounts containing individuals’ personal information. *Id.* Hackers compromised 32,000 LexisNexis customers’ passwords. *Id.* For a complete chronology of recent data breaches, see generally *id.*

disclosure of security breach instances has chilled the public's sense of privacy and its confidence in data collectors.⁴⁹ Each time a database is compromised, identity thieves get their hands on individuals' personal identification information, including names, addresses, social security numbers, and private passwords.⁵⁰ The sheer quantity of people exposed, combined with the potential for economic, social, and psychological harm, justifies the surge of legislative responses.⁵¹ This reaction includes the database security breach notification legislation, which was considered by at least thirty-five states and enacted in twenty-two.⁵²

In light of the growing incidence of breaches and public awareness of them, political pressure has increased to enact legislation addressing identity theft and security breach.⁵³ Both federal and state governments have implemented legislation criminalizing the activities of identity fraudsters.⁵⁴ The focus of identity theft laws has only recently begun to shift from the wrongdoers to those who maintain databases and who, arguably, should bear some responsibility for the protection of consumers' personal information.⁵⁵ However, in order to fully grasp the policy considerations, one must distinguish traditional privacy concerns from modern data protection issues, as they both influence the legal responses to new technology-fueled crimes.

III. PRIVACY VS. DATA CONTROL

When analyzing the effectiveness of recent identity theft legislation, one must keep in mind the distinction between

49. See *infra* notes 218–20 and accompanying text (noting that people who learn that their personal information was exposed via a database security breach typically blame the data holders).

50. See, e.g., Patrick Thibodeau, *Bill Would Force Companies to Disclose Thefts of Personal Data*, COMPUTERWORLD, Dec. 16, 2002, <http://www.computerworld.com/securitytopics/security/privacy/story/0,10801,76768,00.html> (reporting that computer hackers accessed a California state database, containing 265,000 employees' names, social security numbers, and payroll information); see also *supra* text accompanying notes 5–8 (providing examples of breaches that compromised addresses and passwords).

51. See generally FTC Statement, *supra* note 25, at 2–16 (suggesting the need for further legislation to protect against online identity theft).

52. See Nat'l Conference of State Legislatures, 2005 Breach of Information Legislation, <http://www.ncsl.org/programs/lis/cip/priv/breach05.htm> (last visited Jan. 10, 2007) [hereinafter Security Breach Legislation List] (listing security breach disclosure legislation by state).

53. Cf. Nimmer, *supra* note 8.

54. See Solove, *supra* note 16, at 1246–47 (discussing the 1998 Identity Theft and Assumption Deterrence Act, as well as various approaches taken by state legislatures around the country).

55. Skinner, *supra* note 15, ¶¶ 2–3; see also *infra* Part IV (detailing current legislative efforts dealing with identity theft and data security).

traditional “privacy” concerns and modern “data control” or “data protection” issues because conflicting policies often underlie the various types of legislation.⁵⁶ While some of the new laws play a valuable role in modern society, lawmakers must balance one’s right to control the use of private information with another’s right to speak and to use rightfully obtained information.⁵⁷

A. *Distinguishing Privacy from Data Protection*

Privacy and data protection exist as separate and distinct concepts supported by different public policy concerns. The Constitution does not expressly mention privacy, but the Supreme Court recognizes privacy as an implied individual right.⁵⁸ Historically, privacy rights protected the intimate aspects of an individual’s life, such as family relations or embarrassing health issues that, if disclosed, would cause great reputational harm.⁵⁹ Today, privacy rights protect “the individual interest in

56. See Towle, *supra* note 26, at 261–64 (discussing the collision between privacy and identity theft laws).

57. Nimmer, *supra* note 8.

58. See, e.g., *Griswold v. Connecticut*, 381 U.S. 479, 483 (1964) (illuminating the penumbras of the First Amendment that protect individual privacy from intrusion by the government); *Mapp v. Ohio*, 367 U.S. 643, 655–57 (1961) (stating that the Fourth Amendment created a “right to privacy, no less important than any other right carefully and particularly reserved to the people”). Generally, these rights are unique to individuals and are not recognized for businesses or organizations. See NIMMER & TOWLE, *supra* note 2, ¶ 12.02 n.9, at 12-5 (citing numerous cases where courts have held that privacy claims are limited to individuals).

59. See William L. Prosser, *Privacy*, 48 CAL. L. REV. 383, 388–89 (1960). Prosser dissected the right of privacy into four distinct torts: “1. Intrusion upon the plaintiff’s seclusion or solitude, or into his private affairs. 2. Public disclosure of embarrassing private facts about the plaintiff. 3. Publicity which places the plaintiff in a false light in the public eye. 4. Appropriation, for the defendant’s advantage, of the plaintiff’s name or likeness.” *Id.* Clearly, Prosser’s discussion of privacy extended beyond the bounds of this Comment to encompass aspects of privacy law not relevant to identity-theft laws. For cases that limit privacy-law protection to embarrassing or reputationally harmful information, see, for example, *Johnson v. Sawyer*, 47 F.3d 716, 731 (5th Cir. 1995) (considering only the exposed information that was extremely private or embarrassing as part of the potential tort against the plaintiff); *Granger v. Klein*, 197 F. Supp. 2d 851, 868–69 (E.D. Mich. 2002) (“To prevail on a claim that Defendants . . . have published private facts, [the Plaintiff] must show that the disclosed information was highly offensive to a reasonable person and of no legitimate concern to the public.”); *Grimsley v. Guccione*, 703 F. Supp. 903, 909 (M.D. Ala. 1988) (“The Alabama courts have defined the invasion of privacy tort as the wrongful intrusion into one’s private activities in such a manner as either to outrage a person of ordinary sensibilities or to cause such a person mental suffering, shame or humiliation.” (citing *Phillips v. Smalley Maintenance Servs., Inc.*, 435 So. 2d 705 (Ala. 1983))). Despite the historic grounding in protecting people from unsavory revelations of private information, changes appear to be on the horizon in this area of law. See *In re Crawford*, 194 F.3d 954, 958 (9th Cir. 1999) (acknowledging that the Supreme Court’s jurisprudence on this area seems to be in a continual state of flux, stating that although the constitutional “zone of privacy” is judicially well-established, its boundaries are not).

avoiding disclosure of personal matters, and . . . the interest in independence in making certain kinds of important decisions.”⁶⁰ Accordingly, a person has the right to control who has access to and use of his personal information.

Two categories of laws seek to address the two types of protections established by the Court, depending on the type of information at issue. Traditional privacy laws deal with private, “sensitive” information.⁶¹ Data protection laws, however, address more easily obtainable and frequently less sensitive, “personally identifiable information,”⁶² such as telephone numbers or license plate numbers.⁶³

Traditional privacy laws prevent people and governments from obtaining or disclosing an individual’s confidential information, as well as from using that information to harm or discomfit the individual.⁶⁴ These laws are premised on two fundamental concerns: “1) whether the person ha[s] a reasonable expectation of privacy with respect to the information or place, and 2) whether wrongful disclosure would be highly embarrassing to a reasonable person.”⁶⁵

Data protection laws, on the other hand, allow people to assert “obligations of care” and control over their personal identification data in the context of private transactions.⁶⁶ Data control empowers individuals “to determine for themselves when, how, and to what extent information about them is

60. *Whalen v. Roe*, 429 U.S. 589, 599–600 (1977) (footnotes omitted).

61. NIMMER & TOWLE, *supra* note 2, ¶ 12.02, at 12-5.

62. *Id.* Personal identification information is “information that can be directly connected to the individual personally, even if that information is not necessarily sensitive.” *Id.* Interestingly, the laws of the European Union mirror those of the United States on this point. *See* Council Directive 95/46, art. 2(a), 1995 O.J. (L 281) 38 (EC) [hereinafter Data Protection Directive], available at http://ec.europa.eu/justice_home/fsj/privacy/docs/95-46-ce/dir1995-46_part1_en.pdf (part 1) and http://ec.europa.eu/justice_home/fsj/privacy/docs/95-46-ce/dir1995-46_part2_en.pdf (part 2) (defining “personal data” as any information that relates to and directly or indirectly identifies an individual). The Data Protection Directive does not by itself carry regulatory power; rather, it “directs” European Union Member States to enact national laws implementing the goals set out in the Directive. *Id.* pmb. ¶ 20.

63. NIMMER & TOWLE, *supra* note 2, ¶ 12.02, at 12-7 to -8.

64. *Id.*

65. Raymond T. Nimmer, *Contracts, Markets and Data Control* (2005) (unpublished manuscript, available at <http://www.ipinfoblog.com/archives/Stanford-paper-8-1-05.pdf>).

66. Nimmer, *supra* note 8. Information like a social security number, birth date, maiden name, address, and telephone number is often used to prove the identity of an individual and is either a matter of public record or easily discoverable. *See* Towle, *supra* note 26, at 237–38. This type of information is essential for conducting mundane transactions like renting an apartment, cashing a check, or opening a bank account. Even though such information is not per se embarrassing or otherwise “sensitive,” it can be used to the detriment of its owner by identity thieves. *Id.*

communicated to others.”⁶⁷ It gives people a sense of autonomy and freedom of decisionmaking.⁶⁸ Regardless of whether the information has the potential to injure or embarrass, a person should have the right to govern who obtains such information, including whether and how they use it.⁶⁹ Therefore, data control is as much about traditional notions of privacy as it is about the relationships between individuals and businesses that process personal identification data.⁷⁰ The sense of control over personal information allows people to take charge of their own identity and to make self-defining personal decisions.⁷¹

The distinction between issues of traditional privacy and data protection is critical. Traditional privacy laws are ill-equipped to protect nonsensitive information—the dissemination of which has recently become a “privacy” concern. In the recent case of *Busse v. Motorola, Inc.*, customers of a cell phone company filed suit based on the privacy tort of intrusion upon seclusion—a traditional privacy tort action—after the service provider disclosed personal identification information to a research company.⁷² The company retrieved customers’ names, addresses, and social security numbers, then transferred the information to the research company for a study on cell phone use and mortality.⁷³ In deciding whether the disclosure of this data constituted a tort, the court considered whether the facts in question were “private.”⁷⁴ No case law in the jurisdiction supported the contention that publicly available information like a social security number qualified as private.⁷⁵ The court declined to follow the rule adopted in other jurisdictions that recognizes the private nature of social security numbers.⁷⁶ Relying on federal case law, the court instead declared that social security numbers do not constitute private information and therefore dismissed the

67. ALLAN F. WESTIN, *PRIVACY AND FREEDOM* 7 (1967).

68. Edward J. Janger & Paul M. Schwartz, *The Gramm-Leach-Bliley Act, Information Privacy, and the Limits of Default Rules*, 86 MINN. L. REV. 1219, 1247 (2002).

69. Nimmer, *supra* note 8.

70. Nimmer, *supra* note 65 (manuscript at 7).

71. Janger & Schwartz, *supra* note 68, at 1248–49.

72. *Busse v. Motorola, Inc.*, 813 N.E.2d 1013, 1014–15 (Ill. App. Ct. 2004).

73. *Id.* at 1015.

74. *Id.* at 1017–18.

75. *Id.* at 1018.

76. *Id.* For example, a Minnesota Court of Appeals case, *Bodah v. Lakeville Motor Express, Inc.*, looked at the potentially harmful consequences of social security numbers landing in the wrong hands and found the identification numbers to be private, despite the fact that they are not embarrassing in nature. *Bodah v. Lakesville Motor Express, Inc.*, 649 N.W.2d 859, 862–63 (Minn. Ct. App. 2002), *rev'd on other grounds*, 663 N.W.2d 550 (Minn. 2003), *cited in Busse*, 813 N.E.2d at 1018.

suit.⁷⁷ The *Busse* case illustrates the incompatibility between modern data protection and traditional privacy laws. The former seeks to protect an individual's sense of autonomy and to prevent potential losses due to misuse of information, while the latter seeks to protect individuals from reputational harm.⁷⁸

B. Privacy Rights and Freedom of Speech—A Balancing Act

Sometimes, efforts to protect one's privacy rights result in the infringement of another's free speech rights. In these situations, courts must balance the two competing interests carefully. Modern consumer transactions foster disclosure of personal data by individuals and uninhibited use of that information by businesses.⁷⁹ But this sea of information has become a hotbed for crimes like identity theft, prompting a push for data control regulation.⁸⁰

As a general rule, courts refuse to impose liability on companies that disclose individuals' personal data to third parties because American law recognizes the companies' right to speak, disclose information, and to use information freely.⁸¹ For

77. *Busse*, 813 N.E.2d at 1017–18 (citing *Phillips v. Grendahl*, 312 F.3d 357, 373 (8th Cir. 2002) and *Andrews v. TRW, Inc.*, 225 F.3d 1063, 1067 (9th Cir. 2000), *rev'd on other grounds*, 534 U.S. 19 (2001)).

78. *Nimmer*, *supra* note 8, ¶ 2 (outlining the basic juxtaposition of traditional versus modern privacy law); *see also supra* text accompanying notes 64–65 (explaining that privacy jurisprudence centers on protecting individuals from reputational harm).

79. Consumers give sellers credit card numbers; retailers track customers' shopping patterns; and universities use social security numbers for identification purposes. *See, e.g., Laflamme*, *supra* note 2, at S6 (observing that consumers volunteer personal information to obtain retail member cards to buy merchandise at a discount, while retailers use that information to track customer purchasing habits); Personal Experience of Author at University of Houston Law Center (Aug. 2004–May 2007) (being required to use social security number to access university files). In all of these ordinary transactions, individuals generally disclose this information without hesitation. *Cf. Laflamme*, *supra* note 2, at S6 (noting that consumers input information about themselves when shopping online).

80. *See Nimmer*, *supra* note 8, ¶ 1 (“An energetic and effective political move is occurring to create laws that mandate control of so-called ‘personally identifiable’ data.”); *see also* notes 21–22 and accompanying text (providing estimates of the frequency and magnitude of identity theft).

81. *NIMMER & TOWLE*, *supra* note 2, ¶ 12.02, at 12–14 (noting the First Amendment and personal autonomy protect the rights of individuals who obtain information lawfully to use the information); *Nimmer*, *supra* note 8, ¶ 2 (indicating that traditional privacy laws run up against First Amendment concerns). For an example of a court protecting the use of ostensibly “private” information, *see State v. Townsend*, 57 P.3d 255, 260 (Wash. 2002), which held that by voluntarily sending e-mail messages, the defendant impliedly consented to the recording of his communications. Recently, in the context of a motion to suppress evidence, a court determined that information like a defendant's name and address, obtained from the defendant's banking records, did not constitute “private” information and therefore was not protected by the constitutional right to privacy.

example, in *Dwyer v. American Express Co.*, a credit card issuer compiled personal data pertaining to customers' spending habits and rented the information to merchants for advertising purposes.⁸² The credit card holders sued the company under the privacy tort of intrusion of seclusion.⁸³ The court noted that even though Illinois did not recognize the claimed tort, the plaintiffs could not have proved the privacy claim regardless.⁸⁴ The court refused to hold the defendant liable for compiling information, which the plaintiffs voluntarily provided, and then renting the compilation for a lawful use.⁸⁵

At least one court attempted to impose liability for dissemination of contractually acquired information by incorporating modern data control issues into the traditional privacy context. In *Bodah v. Lakeview Motor Express Inc.*, the defendant-employer faxed 204 employees' names and social security numbers to its affiliates in six different states.⁸⁶ Concerned with the risk of identity theft, the employees sued for invasion of privacy by publication of private facts.⁸⁷ The court noted that "social security numbers are not on their face revealing, compromising, or embarrassing. They are, however, such a significant identifier that they . . . can enable someone to impersonate us to our embarrassment or financial loss."⁸⁸ The *Bodah* court held that because of the high risk of harm caused by identity theft, there was some natural expectation of privacy that mandated protection of the information.⁸⁹ This victory was short lived; the Minnesota Supreme Court reversed the decision on grounds that the information was not published, and therefore the elements of invasion of privacy by publication of private facts could not be established.⁹⁰

Courts' refusals to impose liability in situations similar to the *Bodah* case seem understandable given that individuals voluntarily provide information and companies subsequently use

Commonwealth v. Duncan, 817 A.2d 455, 458–59 (Pa. 2003) (finding that the defendant did not have a reasonable expectation of privacy for the personal information obtained from his banking records).

82. *Dwyer v. Am. Express Co.*, 652 N.E.2d 1351, 1353 (Ill. App. Ct. 1995).

83. *Id.* at 1353–55.

84. *Id.*

85. *Id.* at 1354.

86. *Bodah v. Lakeville Motor Express, Inc.*, 649 N.W.2d 859, 860–61 (Minn. Ct. App. 2002), *rev'd on other grounds*, 663 N.W.2d 550 (Minn. 2003).

87. *Id.* at 861.

88. *Id.* at 862. Interestingly, the court used traditional privacy language to describe a data control issue.

89. *Id.* at 862–63.

90. *Bodah v. Lakeville Motor Express, Inc.*, 663 N.W.2d 550, 552 (Minn. 2003).

that information for legitimate purposes. American law recognizes an individual's right to use rightfully acquired information.⁹¹ Hence, if a person possesses information about another individual, that person has the right to use and disseminate the information, unless limited by contracts or confidentiality agreements.⁹² "The fact that information pertains to a specific individual gives that person no claim to control its use."⁹³ This notion of freedom to use knowledge of information is supported by the First Amendment and the concept of "personal autonomy."⁹⁴ Thus, once a person voluntarily provides information to a company, that person should not have the ability to restrict the company's lawful uses of that information.⁹⁵ Perhaps courts fear that without a proper balance between data protection goals and the fundamental right to speak, overly enthusiastic legislation could produce unwanted results.⁹⁶

91. 2 RAYMOND T. NIMMER, *THE LAW OF COMPUTER TECHNOLOGY* § 16:72 (3d ed. 2006).

92. *See id.*

93. *Id.* The right of a party to use information in its possession also applies to "information . . . created by a transaction in which the parties participated"; therefore, grocery stores may track the purchasing habits of customers because the grocer participates in the transaction. *See* NIMMER & TOWLE, *supra* note 2, ¶ 12.05[3], at 12-49.

94. NIMMER & TOWLE, *supra* note 2, ¶ 12.02, at 12-14; *see also supra* note 81 (collecting a series of sources that support this proposition).

95. NIMMER & TOWLE, *supra* note 2, ¶ 12.02, at 12-14.

96. *See* Nimmer, *supra* note 8 (arguing that the restriction of the flow of information produced by privacy laws may result in loss of freedom and innovation that "will outweigh the data protection gain"). The trend in Europe differs drastically from that in the United States. At least one case exemplifies a situation where data protection legislation went too far, in the opinion of the Author. In the case of *Bodil Lindqvist v. Åklagarkammaren i Jönköping*, a Swedish court sanctioned Lindqvist for violating a data protection law when she posted personal information about her colleagues on a church website. Case C-101/01, *Bodil Lindqvist v. Åklagarkammaren i Jönköping*, 2003 E.C.R. I-12971, available at <http://curia.europa.eu/jurisp/cgi-bin/form.pl?lang=en&Submit=Submit&alldocs=alldocs&docj=docj&docop=docop&docor=docor&docjo=docjo&numaff=C-101%2F01&datefs=&datefe=&nomusuel=&domaine=&mots=&resmax=100>. Lindqvist set up an Internet page that was linked to her church's website containing information about the parish and her fellow parishioners, including names, phone numbers, and hobbies. *Id.* At one point, she wrote a posting that stated one of her coworkers had an injured foot and was on half-time leave. *Id.* On appeal, the Swedish court held that the defendant processed personal data in violation of the Data Protection Directive when she referred to her coworkers by name and when she posted information about their health and hobbies. *Id.*; *see also* Data Protection Directive, *supra* note 62, art. 2(b) (defining "processing of personal data").

The outcome of the case is not surprising, considering that when it comes to privacy, Europe has much more stringent laws than the United States. *See* U.S. Dep't of Commerce, Safe Harbor Workbook, sec. I, http://www.export.gov/safeharbor/sh_workbook.html (last visited Jan. 10, 2007) [hereinafter Safe Harbor Workbook] (noting that the U.S. and European laws approach privacy differently). Generally, European privacy legislation is more comprehensive and less concerned with "interfering with the benefits that result from the free flow of information." *Id.* In the United States,

At the same time, the U.S. Supreme Court has not recognized a constitutional right to access information.⁹⁷ Therefore, lower courts are left to find the point of equilibrium somewhere between free access of information and privacy. At least one Federal Court of Appeals has noted:

Although we may feel uncomfortable knowing that our personal information is circulating in the world, we live in an open society where information may usually pass freely. A general level of discomfort from knowing that people can readily access information about us does not necessarily rise to the level of a substantial state interest . . . for it is not based on an identified harm.⁹⁸

The courts have produced uncertain guidance regarding laws that regulate use of information. What about laws that address not the right to use or disseminate properly obtained data, but rather address the level of care taken by the data owner to protect individuals from the risk of identity theft? Lawmakers in this country seem to think it justifiable to impose responsibilities on data owners, as evidenced by the scope and implications of this type of law.

IV. CURRENT DATA PROTECTION LEGISLATION

Legislators attempt to deal with modern privacy and data protection issues on two levels. On one hand, some federal legislation requires organizations collecting personal data to implement security policies and maintain security measures.⁹⁹ On the other hand, as a reaction to security breaches and to the risk of identity theft, some laws mandate prompt public notification of security intrusions in order to apprise consumers of the problem and give them the opportunity to take appropriate remedial actions.¹⁰⁰

Lindqvist's case would have produced a different result. The freedom of speech guaranteed by the First Amendment would likely preempt the coworker's right to prevent Lindqvist from disclosing a foot injury, especially because this kind of information is not embarrassing or private. Nimmer, *supra* note 8, ¶ 4.

97. See BD. OF GOVERNORS OF THE FED. RESERVE SYS., REPORT TO THE CONGRESS CONCERNING THE AVAILABILITY OF CONSUMER IDENTIFYING INFORMATION AND FINANCIAL FRAUD 22 n.20 (1997), available at <http://www.federalreserve.gov/boarddocs/rptcongress/privacy.pdf> ("[T]he Supreme Court does not recognize a constitutional right to information privacy, or a constitutional right of access to information.").

98. U.S. W., Inc. v. FCC, 182 F.3d 1224, 1235 (10th Cir. 1999).

99. See *infra* Part IV.A (detailing some examples of federal legislation that mandates implementation of personal data security policies on data collecting organizations).

100. See *infra* Part IV.B (discussing how state legislation requires data collectors to provide prompt notification alerting data owners following any occurrence of a data

A. *Federal Legislation Requiring the Implementation of Privacy and Security Policies*

In addressing privacy and identity theft problems, the U.S. government has enacted several sector-specific data control laws. These laws oblige organizations that collect or manage consumers' personal data to adopt and implement policies for keeping consumer data secure.

1. *Health Insurance Portability and Accountability Act.* In 1996, the U.S. Congress passed the Health Insurance Portability and Accountability Act (HIPAA),¹⁰¹ which requires the Secretary of Health to establish privacy standards for the maintenance and dissemination of electronically stored health information.¹⁰² The Office for Civil Rights, under the Department of Health and Human Services, enforces the Act through a series of privacy and security rules.¹⁰³ HIPAA applies to healthcare providers that collect and transmit information electronically, insurers, and clearinghouses, as well as to hospitals, health plans, and certain "business associates" of these providers.¹⁰⁴

By and large, HIPAA provisions restrict the disclosure of health information in order to protect the privacy of data subjects.¹⁰⁵ Information qualifies as "protected" by HIPAA if it relates either to the individual's physical or mental condition or to the receipt and payment for care.¹⁰⁶ Identifiable health information may also include an individual's name, social

security breach).

101. Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936, 1936-2103 (codified in scattered sections of Titles 18, 26, 29, and 42 of the United States Code).

102. 42 U.S.C. § 1320d-1(d) (2000), cited in Ethan Preston & Paul Turner, *The Global Rise of a Duty to Disclose Information Security Breaches*, 22 J. MARSHALL J. COMPUTER & INFO. L. 457, 471-73 (2004) (discussing HIPAA and its requirements).

103. U.S. DEPT OF HEALTH & HUMAN SERVS., OFFICE FOR CIVIL RIGHTS, SUMMARY OF THE HIPAA PRIVACY RULE 1 (2003), available at <http://www.hhs.gov/ocr/privacysummary.pdf>.

104. See 45 C.F.R. § 160.103 (2005) (providing definitions, including definitions of "covered entity" and "health plan"). A "business associate" is defined, in part, as a person or entity, other than an employee of a covered member organization, that "performs, or assists in the performance of . . . [an] activity involving the use or disclosure of individually identifiable health information, including claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, billing, benefit management, practice management, and repricing." *Id.*

105. Cf. 45 C.F.R. § 164.504 (2005) (listing use and disclosure restrictions on protected health information).

106. 45 C.F.R. § 160.103 (2005) (defining "[i]ndividually identifiable health information").

security number, birth date, and address.¹⁰⁷ Disclosure of personal identification information is allowed only in limited situations, including when: (1) disclosure is to the individual,¹⁰⁸ (2) disclosure is necessary for treatment,¹⁰⁹ or (3) the individual is given the opportunity to agree or object to the disclosure.¹¹⁰

HIPAA organizations collect individuals' health information for various reasons; the Act focuses on one of these uses, aiming to regulate the "marketing of health information to nonaffiliated third parties by requiring affirmative consent of the individual to make these disclosures."¹¹¹ The Act requires that data subjects receive notice about any disclosures, including to whom the disclosure was made as well as the date of the disclosure.¹¹²

HIPAA focuses on regulating health organizations with regard to use and disclosure of private information without the individual's consent.¹¹³ Although the Secretary of Health and Human Services has provided HIPAA organizations with far-reaching, specific security requirements, none of the regulations explicitly mandates disclosure of security breach to the data subjects.¹¹⁴ There could be an implied duty to disclose security breach, however. The provision requiring notification to data subjects about any "material changes" to disclosure practices may be read to include hostile, unplanned security breaches.¹¹⁵ The "material change" provision coupled with the stringent requirements regarding the collection and disclosure of personal data could imply a duty to notify data subjects about external security breaches.¹¹⁶

Recognizing an implied duty to notify, HIPAA's notice and accounting requirements could be effective in preventing identity

107. *Id.* (specifying information that identifies an individual as falling within the category of protected information); *see also* U.S. DEP'T OF HEALTH & HUMAN SERVS., *supra* note 103, at 3–4 (illuminating the meaning of the statute by providing these specific examples).

108. 45 C.F.R. § 164.502(a)(1)(i) (2005).

109. 45 C.F.R. § 164.502(a)(1)(ii) (limiting this type of disclosure by the provisions of 45 C.F.R. § 164.506 (2005)).

110. 45 C.F.R. § 164.502(a)(1)(v) (conditioning disclosures not otherwise permitted to be made subject to the requirements of 45 C.F.R. § 164.510 (2005), which mandates the affected individual's consent).

111. Steven A. Wells et al., *[Un]Safe Harbor: No Common Denominator in Privacy Compliance*, 9 COMP. L. REV. & TECH. J. 257, 266 (2004).

112. Preston & Turner, *supra* note 102, at 473.

113. *See generally* 45 C.F.R. § 164.510 (2005).

114. *See* Preston & Turner, *supra* note 102, at 475–77 (discussing the implications of current federal legislation, including HIPAA, and noting that the duty to disclose security breaches to data subjects is only implied, and not binding).

115. *See id.*

116. *See id.* (arguing that such a duty is implied).

theft. Once an individual knows that her personal identification information has been disclosed to an unauthorized party, she can take protective measures immediately. However, the enacted legislation addresses only affirmative acts of disclosure by the data holders themselves, not expressly reaching the problem of external security breach or the data holders' responsibilities beyond the breach.¹¹⁷ The mere uncertainty as to such a duty dilutes the thrust of the legislation and its power to fight identity theft resulting from external security breaches.

2. *Children's Online Privacy Protection Act.* The 1998 Children's Online Privacy Protection Act (COPPA)¹¹⁸ empowers the Federal Trade Commission (FTC) to promulgate and enforce rules to protect children's privacy online.¹¹⁹ The Act regulates "unfair and deceptive acts and practices in connection with collection and use of personal information from and about children on the Internet."¹²⁰ COPPA governs only commercial websites and online services that specifically target children.¹²¹ Website operators who *knowingly* collect identification information from children under the age of thirteen must "[p]rovide notice on the website or online service of what information it collects from children, how it uses such information, and its disclosure practices for such information."¹²² However, websites that are not aimed toward children, but which may be accessed by children, do not have to comply with COPPA.¹²³ This loophole allows many children's data to escape unprotected.¹²⁴

COPPA goes beyond merely regulating disclosure of personal identification data, to actually prohibiting the collection of children's personal information without adequate parental consent.¹²⁵ Congress adopted this aggressive embargo on the

117. See *infra* Part IV.B (analyzing security breach notification statutes which address those types of situations).

118. 15 U.S.C. §§ 6501–6506 (2000).

119. 15 U.S.C. §§ 6501–6502 (2000) (defining "Commission" as the FTC and imposing upon that entity the responsibility of promulgating regulations to protect children in this context).

120. 15 U.S.C. § 6502 (2000).

121. 15 U.S.C. § 6501(10) (2000).

122. 16 C.F.R. § 312.3(a) (2006).

123. See NIMMER & TOWLE, *supra* note 2, ¶ 12.11, at 12-75 (pointing out this and other weaknesses of Children's Online Privacy Protection Act (COPPA)).

124. *Id.*

125. See 15 U.S.C. § 6502 (2000) (requiring the FTC to promulgate regulations for operators of websites directed at children, requiring them to obtain verifiable parental consent prior to collection of personal information from children); see also 16 C.F.R.

collection of certain data in order to protect children's identities.¹²⁶ However, lawmakers left the door open for abuse and circumvention of COPPA's intent when they failed to address data collected from children by websites that are not "directed to children."¹²⁷ Moreover, COPPA falls short of addressing the problem of database security breach.¹²⁸ By only regulating disclosure and collection of data, COPPA leaves children whose information has been compromised during a security breach deprived of the opportunity to take curative measures.

3. *The Gramm-Leach-Bliley Act.* In 1999, Congress adopted the Gramm-Leach-Bliley Act (GLBA)¹²⁹ to ensure that financial services providers will safeguard consumers' personal financial information.¹³⁰ The GLBA requires financial institutions to develop and implement data security policies "to prevent the unauthorized disclosure of customer financial information and to deter and detect fraudulent access to such information."¹³¹ These

§ 312.3(b)–(c) (2006) (listing requirements that operators of such websites must fulfill before collecting or maintaining personal information from a child), *quoted in* NIMMER & TOWLE, *supra* note 2, ¶ 12.11, at 12-75 (analyzing obligations of operators of websites covered by COPPA).

126. Marcy E. Peek, *Information Privacy and Corporate Power: Towards a Re-Imagination of Information Privacy Law*, 37 SETON HALL L. REV. 127, 151 (2006).

127. See NIMMER & TOWLE, *supra* note 2, ¶ 12.11, at 12-75.

128. See Preston & Turner, *supra* note 102, at 476–77 (discussing the implications of current federal legislation, including COPPA, and noting that even though it implies a duty to disclose security breaches to affected customers, the statute does not explicitly address the issue of security breaches).

129. Gramm-Leach-Bliley Act of 1999 (GLBA), Pub. L. No. 106-102, 113 Stat. 1338 (1999) (codified in scattered sections of Titles 12 and 15 of the United States Code). Only a portion of this immense statute, dealing with various aspects of the banking, insurance, and securities industries, pertains to this Comment. See Pub. L. No. 106-102, §§ 501–527, 113 Stat. 1338, 1436–50 (1999) (codified at 15 U.S.C. §§ 6801–6827 (2000)).

130. See GLBA, Pub. L. No. 106-102, § 501(a), 113 Stat. 1338, 1436–37 (1999) (codified at 15 U.S.C. § 6801 (2000)) ("It is the policy of the Congress that each financial institution has an affirmative and continuing obligation to respect the privacy of its customers and to protect the security and confidentiality of those customers' nonpublic personal information."). The GLBA empowers the FTC and seven other agencies to promulgate the regulations that states will implement to carry out the purposes of the Act. Wells et al., *supra* note 111, at 270.

131. Hoar, *supra* note 11, at 1435. Specifically, the Act demands that financial institutions implement, as specified by regulations to be promulgated by eight agencies:

administrative, technical, and physical safeguards—

(1) to insure the security and confidentiality of customer records and information;

(2) to protect against any anticipated threats or hazards to the security or integrity of such records; and

(3) to protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer.

15 U.S.C. § 6801(b) (2000).

institutions must present their customers with privacy notices that describe the companies' privacy and data protection policies regarding information disclosure to affiliated and nonaffiliated third parties and to former customers.¹³² These notices must also detail the organization's practices regarding protection of personal identification data from unauthorized use.¹³³ Customers of financial institutions must be given the opportunity to opt out of information disclosures to nonaffiliated third parties.¹³⁴ This element of the legislation allows individuals to retain some control over who obtains their private information.¹³⁵ And finally, the Act prohibits data collection under false pretexts.¹³⁶

The GLBA is a proactive measure intended to reduce identity theft by mandating that financial institutions develop and adopt appropriate data security policies. However, it does not embody a perfect solution to the problem. Financial industry leaders and privacy activists criticize the GLBA as both expensive and ineffective.¹³⁷ While the GLBA aims to safeguard consumers' personal information, the Act fails to state exactly how financial institutions may comply, and the measures that have been explicated have proven largely ineffective in achieving the goal.¹³⁸

132. 15 U.S.C. § 6803(a) (2000); *see also* Janger & Schwartz, *supra* note 68, at 1224–26 (analyzing the notice requirements set out by the privacy provisions of the GLBA).

133. 15 U.S.C. § 6803(a)(1)–(3) (2000). The Act uses the term “nonpublic personal information” and defines the term as “*personally identifiable* financial information—(i) provided by a consumer to a financial institution; (ii) resulting from any transaction with the consumer or any service performed for the consumer; or (iii) otherwise obtained by the financial institution.” 15 U.S.C. § 6809(4)(A) (2000) (emphasis added); *see also* Wells et al., *supra* note 111, at 271 (paraphrasing the statute's definition of personally identifiable data: “any information a consumer provides to obtain a financial product or service, information about a consumer resulting from a transaction to obtain a financial product or service, or information otherwise obtained about a consumer in providing a financial product or service”).

134. *See* 15 U.S.C. § 6802 (2000); *see also* Janger & Schwartz, *supra* note 68, at 1224–26 (discussing the statute's opt-out requirements).

135. Janger & Schwartz, *supra* note 68, at 1226 (explaining that the opt-out requirement protects an individual's “ability to prevent personal information from being shared with non-affiliated companies”).

136. *See generally* 15 U.S.C. § 6821 (2000). The enforcement provisions of the statute include provisions for criminal penalties, agency enforcement, and reports to Congress. 15 U.S.C. §§ 6822–6827 (2000).

137. *See* Janger & Schwartz, *supra* note 68, at 1230–31 (explaining that while industry leaders complain about the expense of privacy notices required by the Act, privacy advocates are at the same time frustrated with the lack of comprehensibility of the privacy notices).

138. *See id.* at 1230–32 (describing the failures of the Act). In addition to using complicated and often confusing language in privacy notices, financial institutions have been known to use tactics designed to discourage consumers from opting-out, making it difficult for consumers to assert their rights. *Id.* at 1231–32. In fact, according to a survey

4. *Fair and Accurate Credit Transactions Act.* The federal Fair and Accurate Credit Transactions Act (FACT) was enacted in 2003 “to prevent identity theft, improve resolution of consumer disputes, improve the accuracy of consumer records,” and to ease consumer access to personal credit information.¹³⁹ FACT governs credit reporting agencies and their reports and scores,¹⁴⁰ but the Act’s “broader application . . . affect[s] essentially every entity engaging in commerce . . . [because] each such business must establish procedures to respond to consumer claims of identity theft.”¹⁴¹ Recognizing that most identity thieves misuse credit accounts, FACT largely focuses on extensions of credit to individuals.¹⁴²

FACT requires the FTC, in consultation with federal banking agencies and the National Credit Union Administration, to provide guidance and regulations to financial institutions on remedial procedures in response to identity theft.¹⁴³ In addition, the Act requires the FTC to implement preventive and protective measures to educate the public on identity theft.¹⁴⁴ Most notably, FACT requires that victims of identity theft be provided with a summary of their rights concerning suspicious credit transactions.¹⁴⁵ As soon as consumers believe they have become victims of identity theft, their rights under FACT are triggered; businesses must then respond by supplying information regarding transactions that took place as a result of identity theft.¹⁴⁶

conducted by the American Banker’s Association, 22% of respondents who received privacy notices did not read them, and 41% were unaware they had received a notice. *Id.* at 1230 (citing Press Release, Am. Bankers Ass’n, ABA Survey Shows Nearly Two Out of Three Consumers Read Their Banks’ Privacy Notices (2001), but using the incorrect title of “ABA Survey Shows Nearly *One* Out of Three Consumers Read Their Banks’ Privacy Notices” (emphasis added) (on file with Houston Law Review)).

139. Fair and Accurate Credit Transactions Act of 2003 (FACT), Pub. L. No. 108-159, 117 Stat. 1952, 1952 (2003) (amending the Fair Credit Reporting Act).

140. See 15 U.S.C. § 1681 (2000) (stating Congress’s findings with respect to credit reports); see also Towle, *supra* note 26, at 269.

141. Towle, *supra* note 26, at 269.

142. See *id.* at 269–70 (describing motivations leading up to the legislation in 2003 and the primary focus of FACT).

143. See 15 U.S.C. § 1681g (2000) (requiring disclosure of the breach to be among the solutions spelled out in agency regulations).

144. *Id.*

145. *Id.*; see also Towle, *supra* note 26, at 279.

146. See 15 U.S.C. § 1681g (2000) (describing the process that is followed when a consumer becomes the victim of identity theft); see also Towle, *supra* note 26, at 279–83 (discussing businesses’ obligations, barring a few exceptions, to supply information to victims upon written request).

The sooner consumer–victims receive information about the theft, the sooner they are able to put an end to the identity theft, thereby minimizing losses. FACT’s emphasis on accurate credit reporting should have a prophylactic effect on privacy and identity theft violations.¹⁴⁷

B. Database Security Breach Notification Statutes

The federal government does not stand alone in adopting creative legislation dealing with the epidemic of identity theft. Individual states have launched assaults on identity theft by enacting legislation to combat the problem.¹⁴⁸ California took an innovative approach when it passed a data security law that shifted the focus from the hackers to those hacked, concentrating on securing the systems that collect and store personal information, by requiring disclosures of security breaches to data owners.¹⁴⁹ Other states have since followed California’s example and enacted similar legislation.¹⁵⁰

1. *The California Model.* California’s Notification Act applies to any person, governmental agency, or business entity conducting business in California and dealing with computerized personal information.¹⁵¹ The law requires these organizations to

147. See generally Maureen A. Young, *New Developments and Compliance Issues in a Security Conscious World*, in 2 SEVENTH ANNUAL INSTITUTE ON PRIVACY LAW: EVOLVING LAWS AND PRACTICES IN A SECURITY-DRIVEN WORLD 347, 355–57 (PLI Intellectual Prop., Course Handbook Series No. G-866, 2006) (providing a detailed analysis of FACT and suggesting the act will be successful).

148. See Security Breach Legislation List, *supra* note 52 (tracking state legislation regarding data security breach across the United States).

149. See CAL. CIV. CODE § 1798.82 (West Supp. 2006) (imposing a duty on businesses to notify California residents immediately following discovery of any breach of system security or unauthorized acquisition of personal information of the consumer and listing acceptable methods for such notification); see also Skinner, *supra* note 15, ¶¶ 2–3 (explaining how California initiated the trend of trying to improve system security, rather than focusing on punishing hackers).

150. See Security Breach Legislation List, *supra* note 52 (reporting that through 2005, at least thirty-five states had introduced security breach notification legislation and at least twenty-two enacted it).

151. CAL. CIV. CODE §§ 1798.29, .82 (West Supp. 2006). The statute 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.

notify promptly “any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person.”¹⁵² The Notification Act covers various forms of security breach,¹⁵³ from physical theft of hard-drive equipment to network penetration by hackers.¹⁵⁴

Once a security breach occurs, the law mandates that the targeted data collectors give notice to the data subjects or data owners¹⁵⁵ “in the most expedient time possible and without unreasonable delay.”¹⁵⁶ Notices of breach are intended to warn potential victims about the data compromise so they can take appropriate remedial measures.¹⁵⁷ The law also aims to encourage data holders to encrypt the information and avoid liability under the statute.¹⁵⁸

Adequate notification of a breach can be accomplished through written, electronic, or substitute notice.¹⁵⁹ A substitute method for notice is appropriate when the organization shows “that the cost of providing notice would exceed two hundred fifty thousand dollars (\$250,000), or that the affected class of subject persons to be notified exceeds 500,000, or the person or business does not have sufficient contact information.”¹⁶⁰ Organizations that suffer a security breach but fail to notify data subjects promptly can be liable for damages.¹⁶¹

CAL. CIV. CODE § 1798.82(e) (West Supp. 2006).

152. CAL. CIV. CODE § 1798.82(a) (West Supp. 2006).

153. The statute defines a breach of security as the “unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the person or business.” CAL. CIV. CODE § 1798.82(d) (West Supp. 2006).

154. See Cheryl A. Falvey et al., *Disclosure of Security Breaches Required by New California Privacy Legislation*, METRO. CORP. COUNS., Aug. 2003, available at <http://www.akingump.com/docs/publication/765.pdf> (reporting the passage of the Notification Act and its requirements and implications).

155. CAL. CIV. CODE § 1798.82(a)–(b) (West Supp. 2006) (stating that database operators who store personal information they do not own have a duty to disclose a security breach to the data owner).

156. CAL. CIV. CODE § 1798.82(a) (West Supp. 2006).

157. See NIMMER & TOWLE, *supra* note 2, ¶ 12.17[3], at 12-122 to -124 (discussing the implications of the legislation).

158. *Id.*

159. CAL. CIV. CODE § 1798.82(g) (West Supp. 2006).

160. CAL. CIV. CODE § 1798.82(g)(3) (West Supp. 2006). Substitute notice may be accomplished by e-mailing the affected person, by posting a notice on the agency’s website conspicuously, or by announcing the breach through statewide media channels. *Id.*

161. CAL. CIV. CODE § 1798.84(b)–(c) (West Supp. 2006). *Cf.* Falvey et al., *supra* note 154, at 5 (stating that “many predict that the disclosure obligation will result in massive class action suits for companies victimized by security breaches”); Laflamme, *supra* note 2, at S6 (reporting that critics of the Notification Act predict the legislation “will unleash a torrent of litigation from injured customers and disgruntled shareholders”).

2. *Goals and Criticism of California's Notification Act.* California's Notification Act has an admirable goal to curb identity theft; however, it remains subject to its own bevy of shortcomings. The most obvious positive result of mandatory breach notification is that early detection of the problem allows customers to minimize their losses.¹⁶² Individuals can cancel compromised credit cards and ask credit bureaus to alert them if suspicious accounts are open in their names.¹⁶³ The knowledge of a potential problem not only allows consumers to take remedial measures but "give[s] them a voice in the decision-making process once their personal information is stolen."¹⁶⁴ However, this positive result has a glaring drawback.

Companies afflicted by database misuse experience embarrassment and fear of losing business, causing them to hide instances of breach from their customers and the public.¹⁶⁵ This fear is not without merit. One survey reports that individuals who learn about a security breach often blame the data holder for failing to protect information and punish the data holder by severing the relationship with that particular organization.¹⁶⁶

Rather than focusing on the potential public relations headaches brought on by breach disclosures, requiring companies to disclose breaches may force businesses and governmental agencies to address security issues proactively and improve security measures. Liability under the Notification Act, coupled with the market forces that punish businesses for irresponsible

162. See Skinner, *supra* note 15, ¶ 20 (noting the strengths of the California law). Early discovery of information misuse may reduce temporal and out-of-pocket expenses incurred. In 2003, the FTC reported that

76% of identity theft victims who detected the identity theft within five months incurred no out-of-pocket expenses, as opposed to only 40% when abuse was discovered after six months or more.

2003 FTC REPORT, *supra* note 22, at 8. Moreover,

76 percent of victims who discovered the misuse of their information within one month spent fewer than 10 hours resolving their problems, while in only 20 percent of cases where it took more than 6 months to discover the misuse were able to resolve all of their problems in less than 10 hours.

Id.

163. See Skinner, *supra* note 15, ¶ 20.

164. *Id.* ¶ 23.

165. See Assembly Comm. on the Judiciary, *S.B. 1386 Bill Analysis*, 3 (June 18, 2002), available at http://www.leginfo.ca.gov/pub/01-02/bill/sen/sb_1351-1400/sb_1386_cfa_20020617_141710_asm_comm.html ("The embarrassment of disclosure that a company or agency was 'hacked,' or the fear of lost business based upon shoddy information security practices being disclosed overrides the need to inform the affected persons.").

166. PONEMON INST., LLC., NATIONAL SURVEY ON DATA SECURITY BREACH NOTIFICATION 2 (2005) [hereinafter SECURITY BREACH SURVEY], available at <http://www.whitecase.com/publications/List.aspx?KeywordPhrase=survey&year=2005> (follow "Security Breach Survey" hyperlink).

security policies, provides strong incentives for organizations to improve data protection voluntarily.¹⁶⁷

In addition, the ambiguous language that peppers the statute has been a major cause of objection to the Notification Act.¹⁶⁸ Critics fear that the vague language of the statute will render the statute useless as technology continues to advance in a way that exacerbates the statute's shortcomings.¹⁶⁹ Critics also argue that undefined essential terms like "unencrypted"¹⁷⁰ and "expedient"¹⁷¹ notice leave businesses wondering whether or not they are complying with the law.¹⁷² This uncertainty forces businesses to be overly cautious or, worse, not cautious enough.¹⁷³ Another criticism of the statute is that while both electronic penetration of a system and physical theft of paper records expose individuals to identity theft, the statute only requires notification in the event of an electronic breach.¹⁷⁴

Many companies are wary because of the statute's potential cross-border implications.¹⁷⁵ The law requires organizations conducting business in California to notify all California residents whose personal information may have been

167. See Preston & Turner, *supra* note 102, at 460 (noting that the market, through consumer behavior, provides incentives for companies to improve their security measures and punishes companies that fail to protect their customers' personal data).

168. See Tyler Paetkau & Roxanne Torabian-Bashardoust, *California Deals with ID Theft: The Promise and the Problems*, BUS. L. TODAY, May/June 2004, at 37, 37 (discussing the abundance of ambiguities in the statute). For a thorough discussion of many of the shortcomings of the Notification Act, see generally Skinner, *supra* note 15, ¶¶ 28–60.

169. Skinner, *supra* note 15, ¶ 32 (arguing that vague definitions of important terms "will make compliance for organizations and enforcement for the courts very difficult").

170. The statute expressly exempts encrypted data from the definition of security breach. See CAL. CIV. CODE § 1798.82(a) (West Supp. 2006) (requiring customer notification if "unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person" (emphasis added)). But the law fails to specify the level of encryption necessary to avoid triggering the statute's notice requirements. Skinner, *supra* note 15, ¶ 45. Thus, even if an organization stores only encrypted data, it cannot be sure that it is not required to provide notice in the event of a security breach. See *id.* (explaining how the lack of specificity may lead organizations to over- or under-invest in encryption technology).

171. CAL. CIV. CODE § 1798.82(a) (West Supp. 2006).

172. Paetkau & Torabian-Bashardoust, *supra* note 168, at 38 (noting the problems caused by ambiguities surrounding the words "unencrypted" and "expedient").

173. *Id.*

174. Skinner, *supra* note 15, ¶ 40.

175. Cf. Paetkau & Torabian-Bashardoust, *supra* note 168, at 37 (describing the Notification Act as a law that "reaches well beyond California's borders, potentially affecting any company, person or agency that has a computer database containing any California resident's 'personal information'"). The question of whether California's reach into interstate commerce encroaches on Congress's power, while interesting and complex, is outside the scope of this Comment.

compromised by a security breach.¹⁷⁶ As written, the statute seems to affect California-based companies that transact business exclusively with California residents, as well as non-California businesses with customers all over the country, including in California.¹⁷⁷

Online merchants, as well as any company keeping personal information on a single California resident will have to comply with the statute.¹⁷⁸ Consequently, the determination of whom to notify following a security breach can become a daunting task for a company that transacts business in all fifty states.¹⁷⁹

The statute gives no guidance regarding how companies should determine whether any individuals affected by a security breach are California residents.¹⁸⁰ This information is not readily available because data collectors do not always amass information pertinent to individuals' residencies; even if they do amass residency information, such information changes frequently.¹⁸¹ Moreover, a multistate company risks public relations and legal complications should it notify California customers but not customers in other states subject to the same security breach.¹⁸² To avoid public disapproval and to limit exposure to liability, companies may be better served to notify all customers without regard to residency status.¹⁸³

Despite its imperfections, the mandatory security breach notification statute has gained popularity.¹⁸⁴ Many other states

176. CAL. CIV. CODE § 1798.82(a) (West Supp. 2006).

177. Paetkau & Torabian-Bashardoust, *supra* note 168, at 39.

178. Skinner, *supra* note 15, ¶ 27.

179. *See id.* ¶¶ 27–28 (noting that practically all online merchants sell goods or services to California residents but few merchants purposefully track the residency of customers).

180. *See* CAL. CIV. CODE § 1798.82 (West Supp. 2006) (lacking a definition of “California resident”); *see also* Skinner, *supra* note 15, ¶ 28 (stating that businesses often do not collect any data that would help them determine the residency of their data subjects).

181. *See* Skinner, *supra* note 15, ¶ 28 (noting that data subjects who were California residents at the time their information was gathered could be residents of a different state at the time of breach, while non-California residents whose information was compromised in a security breach could have become California residents before the breach occurred, thus complicating the notification process).

182. *Id.* ¶ 31; *see also* Paetkau & Torabian-Bashardoust, *supra* note 168, at 39 (warning that non-California residents who were not notified about a security breach may bring negligence claims against a company that notified only California residents).

183. *See* Skinner, *supra* note 15, ¶ 31 (stating that at least one law firm advises companies to “notify every potentially affected data subject in the United States in the event of a breach”).

184. *See* Security Breach Legislation List, *supra* note 52 (chronicling security breach legislation across the United States).

followed California's example and adopted similar legislation.¹⁸⁵ State legislators recognize that notification statutes like California's serve as powerful incentives for businesses to attack identity theft at the front lines.¹⁸⁶

V. SECURITY BREACH NOTIFICATION STATUTES— DO THEY WORK?

The duty to notify consumers about a database security breach imposed by laws like California's Notification Act has its costs and benefits. The successful protection against identity theft outweighs the associated costs.

A. *The Consumers' Perspective*

1. *The Price Paid by Identity-Theft Victims.* Identity-theft victims suffer significant costs. The prevalent results of identity theft are "account takeovers" and "true-name fraud."¹⁸⁷ In an instance of account takeover, the identity thief takes over his victim's existing financial account and attempts to either withdraw cash from a checking account, write checks in the victim's name, or charge purchases to the victim's credit card account.¹⁸⁸ Because the victim receives account statements from the financial institution regularly, victims usually discover account takeovers relatively quickly, giving them the chance to minimize losses.¹⁸⁹ Early detection, however, rests on the assumption that consumers carefully examine account statements, searching for any unusual activity.

185. After the enactment of the Notification Act in California, more than twenty states have followed suit. *Id.*

186. See Skinner, *supra* note 15, ¶ 24 (stating that the California notification statute creates a "powerful incentive to secure data from the beginning"); see also SECURITY BREACH SURVEY, *supra* note 166, at 18 (showing that a majority of people surveyed stated that they were considering or already had discontinued their relationships with an organization after being notified of a data breach).

187. See Jeff Govern, *The Jewel of Their Souls: Preventing Identity Theft Through Loss Allocation Rules*, 64 U. PITT. L. REV. 343, 355 (2003) (describing the two types of identity theft results).

188. Kristen S. Provenza, Comment, *Identity Theft: Prevention and Liability*, 3 N.C. BANKING INST. 319, 320–21 (1999); see also 2003 FTC REPORT, *supra* note 22, at 13 (conveying that 2.4% of survey participants reported misuse of their existing credit card accounts).

189. See Provenza, *supra* note 188, at 320–21 (explaining that victims of "account takeover fraud" discover the fraud in "the following billing cycle, if the account is active," or when "the account becomes past due"); see also 2003 FTC REPORT, *supra* note 22, at 8 (describing the direct correlation between early discovery of identity theft and the expense required to resolve the issue).

Victims of true-name fraud usually suffer greater losses.¹⁹⁰ A true-name fraudster ordinarily “will open new accounts in the victim’s name, but under a different address to avoid alerting the victim.”¹⁹¹ Detection of the crime is inevitably delayed because victims remain unaware for extended periods of time that their identities were stolen.¹⁹² Victims normally do not learn about the crime until they review their credit reports when applying for a home or vehicle loan—which could happen very infrequently.¹⁹³ From this standpoint, notifications alerting individuals of a security breach and the risk of identity theft would have a curative effect.

The development and popularity of the Internet has made consumers even more vulnerable to identity theft.¹⁹⁴ An individual’s “digital biography” consists of one’s name, address, social security number, and other identification information.¹⁹⁵ Various government and commercial organizations assemble these digital biographies for their use, but clever cyber criminals can locate and exploit these biographies.¹⁹⁶ Hackers break into databases containing information about a massive number of people daily, exposing millions of people to the risk of identity theft.¹⁹⁷

To illustrate, one survey suggests that the personal information of 3.25 million Americans, in 2003 alone, was used “to open new credit accounts, take out new loans, or engage in other types of fraud.”¹⁹⁸ This misuse cost victims an average of \$500 per year, and the total annual cost of all forms of identity theft is approximately \$5 billion.¹⁹⁹

Although the consumer costs associated with identity theft in this country are distressingly high, the majority of victims,

190. See Anthony E. White, *The Recognition of a Negligence Cause of Action for Victims of Identity Theft: Someone Stole My Identity, Now Who Is Going to Pay for It?*, 88 MARQ. L. REV. 847, 852 (2005) (explaining how true-name fraud is potentially more damaging than account-takeover fraud).

191. *Id.*

192. *Id.*

193. Hoar, *supra* note 11, at 1425.

194. The vast amount of information available on the Internet gives identity thieves additional avenues to intercept personal identification data. Solove, *supra* note 16, at 1255 (explaining that identity thieves can obtain personal information with relative ease over the Internet).

195. *Id.* at 1254–55.

196. See *id.* (providing detailed information about the architecture of identity theft).

197. See Skinner, *supra* note 15, ¶ 5 (noting that “the average U.S. company’s computer security is attacked by intruders thirty times per week”).

198. 2003 FTC REPORT, *supra* note 22, at 4–5.

199. *Id.* at 6.

surprisingly, do not incur any out-of-pocket expenses.²⁰⁰ Furthermore, surveys indicate that the majority of victims are “not very” or “not at all” worried that they might be victimized again.²⁰¹

2. *Consumers’ Reactions to Database Security Breach Notifications.* The notice requirement of California’s Notification Act and other similar laws purport to give consumers the opportunity to take steps “to protect themselves and their property by taking prompt action to avoid likely fraud.”²⁰² One would think that consumers who learn about a security breach would take all necessary precautionary measures to avoid becoming an identity theft victim, and possibly sustaining substantial monetary losses. As it turns out, however, consumer reactions to breach notification are quite relaxed.²⁰³

The New York law firm of White & Case, LLP, sponsored the first study about breach notifications, conducted by the Ponemon Institute.²⁰⁴ The study found that many consumers who receive security breach notices ignore them, treating them as junk mail.²⁰⁵ Only about half of the respondents that recalled receiving a notice recognized the communication as “an important piece of information”; the other half simply discarded the notices, foregoing the opportunity to take protective measures.²⁰⁶ The study further shows that 50% of the respondents who read the notifications did absolutely nothing to minimize the potential effects of a security breach.²⁰⁷

200. *Id.* at 43 (noting that 63% of identity theft victims incur no out-of-pocket losses).

201. *Id.* at 15 (stating that only 44% of identity theft victims are “very” or “somewhat” concerned that they will become repeat victims). According to the FTC, most identity-theft victims do not report the crime to appropriate authorities and do not notify the credit bureaus about their experiences. *Id.* at 9.

202. Raymond T. Nimmer, Security Breach Notice Laws: Evidence? (Nov. 1, 2005), <http://www.ipinfoblog.com/archives/privacy-data-protection-and-security-35-security-breach-notice-laws-evidence.html>.

203. *See generally* SECURITY BREACH SURVEY, *supra* note 166, at 17 (presenting data that suggests many consumers who learn about security breach take little action to protect themselves from identity fraud).

204. *See id.* at 2 (describing that the study surveyed approximately 50,000 people and received about an 18% response rate).

205. *See id.* at 3 (“Over 39% of respondents initially thought the notice was junk mail, spam or a telemarketing phone call.”).

206. *Id.*

207. *Id.* at 17 (“About 21% say they are monitoring their credit reports more closely, and 9% state that they bought credit monitoring services.”); *see also* 2003 FTC REPORT, *supra* note 22, at 9 (reporting that most victims of identity theft do not report the crime to criminal authorities and do not notify credit bureaus about their experiences).

Of the people affected by a security breach, only some actually become true “victims,” meaning that they suffer some adverse consequence due to the breach; as already stated, the majority of “victims” do not even suffer any financial harm. Therefore, some argue that actual costs incurred by consumers may not be as high as some activists suggest.²⁰⁸ They contend that the media frenzy surrounding security breaches creates an exaggerated picture of the actual state of affairs.²⁰⁹

Even if media reports are more alarmist than perhaps necessary, the potential for devastating losses and the high number of people exposed to that risk call for legislative efforts to curb this emerging crime. Furthermore, even though the majority of consumers suffer little or no out-of-pocket loss, someone else inevitably must bear the costs of identity theft.²¹⁰ Credit card companies and retailers—not the victimized consumers—usually absorb the losses of goods purchased with a stolen identity.²¹¹ And even though security-breach notices do not seem to affect most consumers, they do have an effect on the other side of the spectrum—the entities that are forced to send the notices.

B. The Businesses' Perspective: The Cost and Effects of the Duty to Notify

Businesses are also, and perhaps more so than individuals, victims of security breach.²¹² Notification statutes hold liable the very entities the thieves took advantage of—the businesses—rather than the actual wrongdoers—the hackers who penetrated the systems and exposed individuals to identity theft.²¹³ These

208. See Towle, *supra* note 26, at 254–55 (arguing that media outlets and even regulators give “out of context and quite misleading” reports on the losses incurred by identity theft victims).

209. *Id.*

210. See *id.* at 253–54 (pointing out that consumers generally are not held responsible for the unauthorized misuse of their credit cards and implying the credit card companies may take the brunt of this crime).

211. Holly K. Towle, *Privacy: Identity Theft in the United States*, 5 WORLD INTERNET L. REP. 1, 4 (2004), available at <http://ipinfoblog.com/archives/WILR0804%20towle.pdf> (“Retailers, card companies and others may have suffered some loss even though the ‘victim’ . . . did not.”).

212. See Nimmer, *supra* note 202, ¶ 7 (stating that companies are the “actual victim”).

213. See, e.g., CAL. CIV. CODE § 1798.82 (West Supp. 2006) (addressing actions by data collectors and remaining silent with regard to hackers). Various criminal statutes punish the actual wrongdoers—the hackers who compromise the companies’ security systems. See, e.g., CAL. PENAL CODE § 502 (West 1999 & Supp. 2007) (prescribing criminal penalties for various breaches of computer systems including use of stolen data); MD. CODE ANN., CRIM. LAW § 7-302 (LexisNexis 2002) (same); N.J. STAT. ANN. § 20:25 (West

laws impose the costs of notifying at-risk individuals on businesses and other organizations collecting personal identification data.²¹⁴

These expenditures reach beyond just the cost of sending out notifications. The lawmakers forced database holders to adopt more aggressive security policies and procedures to protect customer information.²¹⁵ Accordingly, these statutes implicitly require companies to spend money on encryption mechanisms, intrusion detection devices, firewalls, and other hacking defense technology.²¹⁶

Commercial organizations pay another larger price as a result of mandatory breach notifications—loss of business. One business leader believes that “[t]he protection of a firm’s reputation and brand is directly linked to the secure management of data, the applications that use that data, its people and assets.”²¹⁷ Disclosure of a security breach tarnishes a company’s public image.

According to the Ponemon Institute, individuals who receive breach notices “blame the organization for not having sufficient controls or safeguards to protect their data . . . [and] are likely to lose trust and confidence in the organization.”²¹⁸ Nineteen percent of the respondents in the survey ended their relationship with the company, and another 40% were considering termination.²¹⁹ These numbers clearly suggest the impact of

2005) (same); TEX. PENAL CODE ANN. § 33.02 (Vernon 2003 & Supp. 2006) (same); *see also* Nimmer, *supra* note 202, ¶ 8.

214. *See, e.g.*, CAL. CIV. CODE § 1798.82 (West Supp. 2006) (requiring data collectors to send out notices of security breach).

215. *See* Chad C. Coombs & Keenen Milner, *Practice Tips: New California Identity Theft Legislation*, L.A. LAW., July/Aug. 2004, at 21, 21 (discussing the Notification Act and its impact on businesses).

216. *See id.* at 24–25 (recommending that companies affected by the Notification Act install measures as defense mechanisms against security breach); *see also* CAL. DEPT OF CONSUMER AFFAIRS, RECOMMENDED PRACTICES ON NOTICE OF SECURITY BREACH INVOLVING PERSONAL INFORMATION 5 (2006), *available at* <http://www.privacyprotection.ca.gov/recommendations/secbreach.pdf> (“Implementing an effective information security program is essential for an organization to fulfill its responsibilities towards the individuals who entrust it with their personal information.”).

217. Pizzo, *supra* note 4, at 9 (quoting Cal Slemple, IBM Global Services, Vice President of Security and Privacy Services).

218. SECURITY BREACH SURVEY, *supra* note 166, at 2.

219. *Id.* at 3. Another study found that, in 2002, publicly-traded companies “lost 2.1% of their market value within two days” of a security breach disclosure. Preston & Turner, *supra* note 102, at 491 (citing Huseyin Cavusoglu et al., *The Effect of Internet Security Breach Announcements on Market Value: Capital Market Reactions for Breached Firms and Internet Security Developers*, 9 INT’L J. ELECTRONIC COM. 69, 71 (2004)).

disclosure outweighs the potential legal liabilities imposed through the notification statutes.²²⁰

The method used for notification also affects customers' reactions to breach notices. The Ponemon Institute reports that companies that call their customers or use personalized letters are three times less likely to lose customers than companies that merely send out mass e-mails or form-letter notifications.²²¹ If a company wants to preserve relationships with customers, it appears that the company should choose the more expensive personalized methods of providing notice. Additionally, consumers believe that an organization should report a security breach regardless of whether the compromised data was encrypted or unencrypted,²²² which puts pressure on businesses to spend money on notifications even when they are not required to do so by law.²²³

Finally, instances of security breach that make the headlines expose the business–victims of security breach to additional embarrassment and public contempt.²²⁴ Naturally, to avoid all of these costs, companies are compelled to change their privacy policies and improve their database security safeguards.

C. *The “Invisible Hand” Effect*

One privacy law expert associates the consequences produced by the breach notification statutes with Adam Smith's “invisible hand” effect:²²⁵ “Each business independently looks after its own interests by imposing the level of security it believes necessary to insulate it from liability,” the net result being

220. Raskopf & Bender, *supra* note 1, at 5.

221. SECURITY BREACH SURVEY, *supra* note 166, at 3.

222. *Id.* at 4 (stating that 82% of respondents thought that companies should report a breach even if the information contained in the accosted database was encrypted). However, only 22% of participants knew what encryption was. *Id.* at 12.

223. *Cf.*, CAL. CIV. CODE § 1798.82(a) (West Supp. 2006) (requiring disclosure of a security breach only if the system contains unencrypted data).

224. *See* Raskopf & Bender, *supra* note 1, at 5 (noting the growing amount of media attention given to data security breaches); David Wichner & Thomas Stauffer, *Data Breach Imperils 90 Local Jobs*, ARIZ. DAILY STAR, July 23, 2005, at D1 (arguing that the market pressures businesses into spending more than they are required by law); *see also* Towle, *supra* note 26, at 254–55 (discussing the negative attention generated in the media surrounding security breaches).

225. Nimmer, *supra* note 202, ¶ 15 (applying the concept of the invisible hand to this context); *see also* ADAM SMITH, AN INQUIRY INTO THE NATURE AND CAUSES OF THE WEALTH OF NATIONS 291–92 (Kathryn Sutherland ed., Oxford Univ. Press 1998) (1776) (“[B]y directing . . . industry in such a manner as its produce may be of the greatest value, he intends only his own gain, and he is in this, as in many other cases, led by an invisible hand to promote an end which was no part of his intention.”).

“foster[ing] the public welfare.”²²⁶ Even if the notification statutes did not impose legal liability, the requirement of notification itself is proving a powerful incentive for data collectors to develop appropriate levels of security.²²⁷ The mere risk of negative publicity associated with giving notice to consumers motivates companies to improve their data security practices voluntarily—the invisible hand truly at work.²²⁸

U.S. lawmakers have long relied on industry’s self-interest as a means to naturally regulate privacy issues.²²⁹ Policymakers recognize that market incentives provide a healthy balance between the value businesses put on collecting data and the value individuals place on keeping control over their personal information.²³⁰ Meanwhile, the fear of eroding “societal benefits brought about by new technologies and the free flow of information”²³¹ has prevented the federal government from enacting broad-based privacy rules that are prevalent in Europe.²³²

The United States and Europe approach privacy regulation differently. European nations recognize privacy as a fundamental human right and have a long “tradition of prospective, comprehensive lawmaking that seeks to guard against future harms, particularly where social issues are concerned.”²³³ Privacy in the United States, however, is not absolute, and U.S. laws

226. David Bender, Data Protection and Privacy Law Update 2006, <http://www.infolaw.org/2006slides.htm> (follow “Data Protection & Privacy Law Update 2006” hyperlink) (on file with the Houston Law Review), *cited in* Nimmer, *supra* note 202, ¶ 15 (paraphrasing Mr. Bender’s argument: “Even in the absence of any litigation or liability, the statutes themselves and the risk of being required to give notice, have created strong incentives for businesses to develop levels of security appropriate to the type of data they hold”).

227. *See* Preston & Turner, *supra* note 102, at 460 (“Customers will be reluctant to transact with businesses that fail to adequately secure their databases.”); *see also supra* Part V.B (evaluating costs borne by organizations forced to notify customers about security breaches).

228. Nimmer, *supra* note 202, ¶ 15.

229. *See* James P. Nehf, *Incomparability and the Passive Virtues of Ad Hoc Privacy Policy*, 76 U. COLO. L. REV. 1, 2, 44–45 (2005) (noting that U.S. information-privacy laws favor self-regulation principles over broad-based privacy rules employed by European governments).

230. *Id.* at 18–19. “Many businesses will collect a minimum amount of customer data and keep it secure in order to avoid negative publicity . . .” *Id.* at 18. Businesses may also attract “customers from competitors whose data collection and sharing policies are less protective.” *Id.* at 19.

231. *Id.* at 2.

232. *See generally* Data Protection Directive, *supra* note 62, art. 25 (mandating European Union states to adopt specific privacy legislation and prohibiting transfer of personal data to nonmember countries that do not have comparable standards).

233. Safe Harbor Workbook, *supra* note 96, at sec. I.

preserve a balance between an individual's need to control personal information and society's benefit from using this type of information.²³⁴ The United States therefore has resisted the broad-sweeping approach to privacy regulation, preferring instead a more market-driven and industry-regulated approach.²³⁵

Admittedly, pure self-regulation is not a perfect model to protect consumers from privacy invasion and identity theft.²³⁶ The "cost-benefit approach to privacy" is less than perfect when businesses miscalculate the value people place on privacy as compared to other competing interests.²³⁷ But notification statutes complement the self-regulation model by increasing the stakes for data collectors. Mandatory breach notifications inflict on businesses costs associated with both a tarnished image and the expense of providing notice. These elevated costs provide more motivation for companies to ensure proper consumer data protection. By acting to reinforce the market-driven desire to provide customers with a sense of security, notification statutes provide an effective tool to curb database security breaches and identity theft.

VI. SUGGESTING A FEDERAL NOTIFICATION STATUTE FOR UNIFORM NATIONWIDE IMPLEMENTATION

Having concluded that security breach notification statutes effectively deal with database security breach and identity theft, the next logical conclusion is that a uniform federal law best implements this legislative device nationwide.

Whether intended or not, California's Notification Act has cross-border implications.²³⁸ With a growing population of 37 million and an economy roughly the size of France, California is a desirable place of business.²³⁹ In fact, any national (or even multistate) company that conducts business in the United States will likely conduct business in California.²⁴⁰ Thus, many

234. Jonathan P. Cody, Comment, *Protecting Privacy Over the Internet: Has the Time Come to Abandon Self-Regulation?*, 48 CATH. U. L. REV. 1183, 1202-03 (1999).

235. Safe Harbor Workbook, *supra* note 96, at sec. I.

236. See generally Budnitz, *supra* note 14, at 848 (arguing that pure self-regulation inadequately protects consumer privacy in electronic transactions).

237. Nehf, *supra* note 229, at 4 (using the phrase "cost-benefit approach to privacy" to refer to the market-orientation that characterizes data control laws in the United States).

238. See *supra* notes 175-77 and accompanying text (considering the law's ramifications for non-California based businesses).

239. Bender, *supra* note 226.

240. *Id.*; see also Avivah Litan & John Pescatore, *Stolen Credit Card Case Should*

companies must comply with California's security breach notification statute.

After California set a "national trend" by enacting the Notification Act,²⁴¹ about thirty states embraced the trend, adopting their own security breach notification statutes that also have potential cross-border implications.²⁴² Unfortunately for businesses, these laws are not uniform.²⁴³ For instance, key terms like "personal information" are not consistently defined, creating discrepancies as to whether a company must disclose a security breach.²⁴⁴ Other important differences among these laws include the triggering of substitute notification and consumer remedies.²⁴⁵ Consequently, companies doing business in multiple states must review each of the statutes that might apply and develop costly and overlapping compliance mechanisms.²⁴⁶

Federal legislation like the GLBA further contributes to the compliance nightmare.²⁴⁷ For example, most of the notification statutes exempt organizations that keep consumer data in an encrypted format,²⁴⁸ but the GLBA does not.²⁴⁹ Thus, the expenditures that a financial institution incurs to comply with

Prompt Card Companies to Act, GARTNER, Feb. 20, 2003, <http://www.gartner.com/resources/113200/113282/113282.pdf> (noting that virtually all online merchants do business in California).

241. Paetkau & Torabian-Bashardoust, *supra* note 168, at 41.

242. See generally Security Breach Legislation List, *supra* note 52 (reporting that at the beginning of 2004 the only breach notification statute in the country was California's, that at least twenty-two states passed breach notification statutes in 2005, and that at least twelve were passed in 2006). Similar breach notification legislation is pending in the majority of the remaining states. *Id.* (stating that "[l]egislation [has been] introduced in at least 31 states in 2006," 12 of which had enacted the statutes as of September 14, 2006).

243. See Holly K. Towle, *Proliferation of Information Security Breach Notification Statutes*, July 21, 2005, <http://www.klgates.com/newsstand/Detail.aspx?publication=3282> (considering the differences between states' security breach notification statutes).

244. See *id.* (giving a detailed comparison and contrast of how security breach notification statutes in California, Georgia, Montana, and North Dakota define "personal information").

245. Compare COLO. REV. STAT. § 6-1-716(1)(C)(IV) (2006) (permitting substitute notice by various electronic and print media if certain conditions, for example more than 250,000 persons to be notified, are met), with CONN. GEN. STAT. ANN. § 36a-701(b)(e)(4) (West Supp. 2006) (allowing substitute notice if certain conditions, including that more than 500,000 persons need to be notified); compare also MICH. COMP. LAWS ANN. § 445.71 Sec. 11(2) (West Supp. 2006) (punishing a knowing violation with up to thirty days imprisonment, a fine of up to \$1,000, or both), with TENN. CODE ANN. § 47-18-2105(d) (2001) (setting civil monetary penalties, the minimum of which is \$10,000, in addition to any other remedies available under consumer protection statutes).

246. See Towle, *supra* note 243.

247. *Id.* (giving examples of confusion between parallel sections of the California Breach Notification Statute and the GLBA).

248. See, e.g., CAL. CIV. CODE § 1798.82(a) (West Supp. 2006) (requiring breach notification only when *unencrypted* data is compromised).

249. Towle, *supra* note 243.

the California notification statute do not necessarily bring the company into compliance with the GLBA.²⁵⁰

Notification statutes effectively curtail identity theft because the costs involved with public notification induce companies to implement more responsible security measures. However, the current hodge-podge of legislation with multistate implications poses a threat to the viability of data collecting businesses.²⁵¹ This threat transforms the statutes from tools that foster useful market forces in terms of stimulating more responsible data handling into misfits that produce an environment of uncertainty, undermining companies' efforts to comply.

The benefits of security breach notification statutes can be reclaimed by a federal security breach notification statute.²⁵² As written, the California statute is not the perfect model for such legislation because it still contains ambiguities that need to be addressed.²⁵³ However, it is a good starting point, with the potential to infuse improved data security and reduce identity theft without over-regulating businesses. The corporate self-regulation approach favored by the current administration has not been able to keep up with the recent explosion of identity fraud.²⁵⁴ And the existing state notification statutes expose multistate corporations to increased liability.²⁵⁵ A uniform law offers the logical and practical next step.²⁵⁶

250. See *id.* Moreover, the GLBA applies only to "financial institutions." See *supra* note 131 and accompanying text.

251. Cf. Towle, *supra* note 243 (acknowledging that businesses that sustained expenses to comply with the California statute are having to incur additional expenses every time a new state law is passed).

252. Legislation similar to California's Notification Act is already pending in the U.S. Senate. S. 3713, 109th Cong. (2006); see also Paetkau & Torabian-Bashardoust, *supra* note 168, at 41; Richard S. Eisert, *Security Breach Notification Laws Become the Statutory Norm*, METROPOLITAN CORP. COUNS., Aug. 2006, at 13, 13 n.1 ("In June 2006, Sen. Clinton introduced . . . the PROTECT ('Privacy Rights and Oversight for Electronic and Commercial Transactions Act of 2006') Act. Among the bill's far-reaching provisions are a national requirement for immediate security breach notification . . ."); Posting of Shannon Kellog, *Breach Notification/Data Security Legislation Top of Mind in the U.S.—Americans Want Action, Speaking of Security*, <http://www.rsasecurity.com/blog/entry.asp?id=1102> (May 25, 2006) (reporting that key committees in the House of Representatives have passed two federal breach notification bills, both of which include exemptions for encrypted information).

253. See Skinner, *supra* note 15, ¶ 69 (concluding that California's security breach notification statute is not ready "to serve as the final template for national breach notification legislation"); see also *supra* Part IV.B (explicating criticisms of the statute).

254. Skinner, *supra* note 15, ¶ 60.

255. *Id.* ¶ 61 (explaining that the existence of different breach notification statutes could create a scenario in which "organizations that do business nationwide will be buried in an avalanche of what could be conflicting obligations").

256. See *id.* (implying that a national bill would help to "avoid this feared piecemeal approach").

VII. CONCLUSION

Computer security breaches occur at an alarming rate, exposing millions of Americans to the risk of identity theft. By exploiting computer system security vulnerabilities, identity crooks prosper, trafficking in all kinds of consumer information stored in databases maintained by business and governmental organizations. Legislation that mainly focuses on prosecuting hackers and identity thieves can no longer keep up with the rapid growth of identity theft. Thus, the spotlight must shift to those who collect and store consumer personal information and fail to protect it from criminals.

Security breach notification statutes like California's ensure that consumers are protected from identity thieves. These laws expose database holders who fail to protect consumer data to civil liability, monetary losses, increased employee efforts, a tainted public image, and loss of business opportunities. Even though breach notification statutes affect entities that are themselves victims, the benefits created by imposing such harsh consequences onto businesses far outweigh the costs. Out of the two victims—the consumer and the corporation—the latter is better equipped to influence changes that could benefit both groups.

The duty to notify consumers about security breach inflicts tremendous cost on businesses. These costs inevitably induce behavioral changes that result in more sound privacy policies and improved database-security safeguards—thereby reducing identity theft.

To ensure that this concept is implemented nationwide, and to ease companies' efforts to comply, a uniform federal law requiring notification of security breach is an appropriate solution. A federal law requiring consumer data collectors to disclose instances of security breach would provide powerful market incentives for tighter data security and diminish identity fraud. This type of legislation would force companies to assess what appropriate security measures are needed in order to avoid liability, and, in the process, protect consumer data from identity thieves.

Lilia Rode