THE EMERGENCE OF STATE DATA PRIVACY AND SECURITY LAWS AFFECTING EMPLOYERS

Joseph J. Lazzarotti[*]

SUMMARY

Identity theft is becoming the fastest growing criminal offense in the United States.[1] States have been more aggressive than the federal government in mandating protections for the kinds of personal information thought to be more likely to enable identity theft.[2] These

[*] Joseph J. Lazzarotti is a Partner with Jackson Lewis LLP, in the firm's White Plains, NY office. He heads the firm's HIPAA and Workplace Privacy Practice Group and advises companies regularly regarding data privacy and security issues nationally and internationally. He also counsels companies with respect to compliance issues related to their retirement and welfare plans under ERISA, HIPAA, the Internal Revenue Code and other federal statutes. A substantially similar version of this article was originally published on lexis.com as an Emerging Issues Commentary, Lazzarotti on State Data Privacy and Security Laws. For more insightful articles on the latest cases, statutes and legal developments, see lexis.com at Legal>Secondary Legal>Expert Commentaries.

1. *Holding the Department of Homeland Security Accountable for Security Gaps, Before the H. Comm. on Homeland Security.*, 110th Cong. 20 (2007) (testimony of Hon. Michael Chertoff, Secretary, U.S. Department of Homeland Security), *available at* http://homeland.house.gov/SiteDocuments/20070905140841-10943.pdf; Cathy Zollo, *An Identity Trove Intact in the Trash: Man Finds Potential Bonanza for Thieves Behind a Sarasota Store*, SARASOTA HERALD-TRIB. (Fla.), Oct. 23, 2007, at A1; Press Release, Ill. Sec'y of State, Jesse White Unveils New Driver's License and ID Card Featuring State-of-the-Art Security (Oct. 23, 2007), *reprinted in Secretary of State White Unveils New Driver's License, Identification Card Featuring State-of-the-Art Security*, U.S. ST. NEWS, Oct. 23, 2007; *see* Eric Gillen, *Protecting Yourself Against Identity Theft*, THE STREET.COM, Feb. 27, 2002, http://www.thestreet.com/markets/ericgillin/10010609.html (last visited Sept. 28, 2008).

2. *Compare, e.g.*, CAL. LAB. CODE § 226 (West Supp. 2008) ("[B]y January 1 2008, only the last four digits of [the employee's] social security number or an . . . employee identification number other than a social security number may be shown on the . . . itemized statement."), HAW. REV. STAT. §§ 487-1 to -16, 487J-1 to -4, 487N-1 to -4, 487R-1 to -4 (1993 & Supp. 2007) (providing for protection of: the consumer and a person's social security number, an individual's information in the event of a security breach, and a person's information when records containing this information are disposed), MASS. CODE REGS. § 17.03 (2008) (creating a requirement for all businesses maintaining personal information on a Massachusetts resident to adopt and implement a

rapidly emerging state mandates generally apply to all businesses operating in the state and to a broad set of personal information.[3] Of particular concern for businesses is how these statutes apply to the personal information they maintain about their employees.[4]

I. INTRODUCTION

Reports of breaches of personal information affecting hundreds or thousands, if not millions, of individuals regularly occupy the news media.[5] Instances of stolen laptops and PDAs, unauthorized entries into electronic data bases and similar attacks on personal information are frequent and affect large numbers of people.[6]

Since 2005, over 245 million records containing personal information are reported to have been involved in security breaches in the United States.[7]

The Federal Trade Commission ("FTC") reported that calendar year

comprehensive, written information security program), N.J. STAT. ANN. §§ 56:8-161 to :8-166 (West Supp. 2007) (mandating certain actions which will further the goal of protection of an individual's personal information), *and* N.Y. GEN. BUS. LAW §§ 399-dd, -h (McKinney Supp. 2008) (providing: restrictions intended to ensure that an individual's social security number remains confidential and standards for the manner in which personal information is to be disposed), *with* 15 U.S.C.A. § 6801 (West Supp. 2007) (regarding the safeguards to be taken by financial institutions to ensure that the information of a customer that is not public, remains secure), 16 C.F.R. § 682.3 (2007) (setting a standard that must be met when a person is disposing of the information of a consumer), 29 C.F.R. § 825.500(g) (2006) (providing that certain medical records and documents required by the Family Medical and Leave Act are to be kept in a confidential manner, separate from the employee's other records), 29 C.F.R. § 1630.14(c)(1) (2007) (providing that employee information gathered during a medical examination of that employee is to be kept in a confidential manner, separate from the employee's other records), *and* 45 C.F.R. § 164 (2007) (providing security and privacy standards for the health care entities covered under these provisions).

3. *See, e.g.*, CAL. LAB. CODE § 226 (West Supp. 2008); HAW. REV. STAT. §§ 487-1 to -16, 487J-1 to -4, 487N-1 to -4, 487R-1 to -4 (1993 & Supp. 2007); N.J. STAT. ANN. §§ 56:8-161 to :8-166 (West Supp. 2007); N.Y. GEN. BUS. LAW §§ 399-dd, -h (McKinney Supp. 2008).

4. *See generally* Richard Alaniz, *Striking the Balance: MVR Checks and Privacy Laws*, WORK TRUCK ONLINE, Feb. 2008, http://www.worktruckonline.com/Channel/New-Fleets/Article/Story/2008/02/Striking-the-Balance-MVR-Checks-and-Privacy-Laws.aspx (last visited Sept. 28, 2008) (mentioning the difficulties businesses can face when trying to comprehend and obey the federal and state laws that have been passed to protect the personal identity information of individuals).

5. *See* PRIVACY RIGHTS CLEARINGHOUSE, A CHRONOLOGY OF DATA BREACHES (2008), http://www.privacyrights.org/ar/ChronDataBreaches.htm (last visited Nov. 14, 2008) [hereinafter A CHRONOLOGY OF DATA BREACHES]; *see, e.g.*, Zollo, *supra* note 1, at A1; Gillin, *supra* note 1; Will Sturgeon, *Could Your Laptop Be Worth Millions?*, C-NET NEWS.COM, Jan 27, 2006, http://www.news.com/Could-your-laptop-be-worth%20-millions/2100-1029_3-6032177.html (last visited Sept. 28, 2008).

6. Sturgeon, *supra* note 5.

7. A CHRONOLOGY OF DATA BREACHES, *supra* note 5.

2007 was the eighth consecutive year in which identity theft was the principal complaint the agency received.[8]

According to a 2006 CSI/FBI Survey, 52% of company respondents reported an "unauthorized use of [their] computer systems" during the past 12 months.[9]

The cost of a data breach can be staggering: the average laptop contains data worth approximately $972,000[10] and, according to a Federal Bureau of Investigation Computer Crime Survey, the average annual cost of computer security incidents is $67.2 billion.[11] The problem has shown no sign of slowing.[12]

What has emerged in the United States to counter this growing threat is a patchwork of state and federal statutes and regulations that focuses on punishing wrongful accesses to, and uses and disclosures of, personal information.[13] This patchwork generally requires that preventive steps be taken to minimize such accesses, uses, and disclosures.[14] While the majority of reported data breaches involve

8. Press Release, Fed. Trade Comm'n, FTC Issues Annual List of Top Consumer Complaints (Feb. 13, 2008), www.ftc.gov/opa/2008/02/topcomplaints.shtm (last visited Nov. 14, 2008). For 2007, 32% of all 813,899 complaints received by the FTC related to identity theft, or 258,427. *Id.*

9. LAWRENCE A. GORDON ET AL., THE 2006 CSI/FBI COMPUTER CRIME AND SECURITY SURVEY 10-11 (2006), http://i.cmpnet.com/gocsi/db_area/pdfs/fbi/FBI2006.pdf (last visited Sept. 28, 2008).

10. Sturgeon, *supra* note 5.

11. Joris Evers, *Computer Crime Costs $67 Billion, FBI Says*, CNET NEWS.COM, Jan. 19, 2006, http://news.com.com/Computer+crime+costs+67+billion%2C+FBI+says/2100-7349_3-6028946.html?tag=nl (last visited Sept. 28, 2008).

12. Mark Jewellap, *Record Number of Data Breaches in 2007, Upward Trend of Stolen Personal information Expected to Continue*, MSNBC.COM, Dec. 30, 2007, http://www.msnbc.msn.com/id/22420774/ (last visited Sept. 28, 2008).

13. *See A Review of State and Federal Privacy Laws: Testimony to the California Leg. J. Task Force on Personal Information and Privacy* (Ca. 1997) (testimony of Beth Givens, Project Director, Privacy Rights Clearinghouse) (Apr. 1, 1997), http://www.privacyrights.org/ar/jttaskap.htm (last visited Sept. 28, 2008); *see also* Alaniz, *supra* note 4 (discussing the laws that have been enacted—both federally and by various states—to safeguard personal information).

14. *See, e.g.*, OR. REV. STAT. ANN. § 646A.622(1) (West Supp. 2008) ("Any person that owns, maintains or otherwise possess data that includes a consumer's personal information that is used in the course of the person's business, vocation, occupation or volunteer activities must develop, implement and maintain reasonable safeguards to protect the security, confidentiality and integrity of the personal information, including disposal of the data."); MD. CODE ANN., COM. LAW § 14-3503(a) (West Supp. 2007) ("a business that owns or licenses personal information of an individual residing in the State shall implement and maintain reasonable security procedures and practices that are appropriate to the nature of the personal information owned or licensed and the nature and size of the business and its operations."); 2008 Conn. Acts No. 08-167 (Reg. Sess.) ("Any person in possession of personal information of another person shall safeguard the data, computer files and documents containing the information from misuse by third parties, and shall destroy, erase or make unreadable such data, computer files and documents prior to disposal.").

consumer data,[15] businesses also must take stock of the sensitive personal information they possess regarding their employees and their employees' families. As employers, businesses are massive repositories for and frequent transmitters of sensitive personal information.[16] Accordingly, businesses and practitioners should be mindful of the entire spectrum of personal information an organization might own, maintain, or have access to in developing safeguards for the access, use, maintenance, disclosure, and destruction of personal information.

This commentary discusses the emerging legislative and regulatory developments and, in particular, how they relate to employee personal information. To date, the federal government has taken a limited, somewhat "silo-like" approach to protecting personal information.[17] It has selected only certain types of employee information as worthy of protection.[18] However, the states have enacted broadly applicable mandates to safeguard wider classifications of information.[19] As a result, for practitioners representing businesses with operations in more than one state, the task of providing guidance becomes more complex and the risk of liability for those businesses compounds.

II. SUMMARY OF KEY DATA PRIVACY AND SECURITY MEASURES

A. International Law

Though the focus of this commentary is on United States law, businesses and practitioners cannot ignore the data privacy and security mandates abroad. In most cases, foreign laws are more stringent than those in the United States.[20] For example, an American parent company may find it difficult to obtain certain information about its employees

15. *See* Jewellap, *supra* note 12.

16. *See* Alaniz, *supra* note 4 (noting the immense amount of personal information employers can come to possess when performing motor vehicle record checks on their employees).

17. *See Privacy Breach Exposes on the Uptick; Know What the Risks Are: Panel Recap from PLUS 2008 Professional Risk Symposium on May 7, 2008*, 21 PLUS J. REPRINT (Professional Liability Underwriting Society, Minneapolis, M.N.), June 2008, *available at* http://www.crslimited.com/news/articles/Privacy%20Breach%20-%20Recap%20PRS%20Reprint.pdf.

18. *See infra* notes 29-35 and accompanying text.

19. *Compare infra* notes 29-35 and accompanying text (describing federal government requirements for protection of employee information), *with infra* notes 91-95 and accompanying text (describing various state requirements for protection of employee information).

20. *See* Bob Sullivan, *Privacy Lost: EU, U.S. Laws Differ Greatly*, MSNBC.COM, Oct. 19, 2006, http://www.msnbc.msn.com/id/15221111/ (last visited Sept. 28, 2008).

working in other countries.[21] Many other countries do not permit employers to diminish an employee's expectation of privacy in the workplace and view this country as not having adequate data protection.[22] Thus, businesses and practitioners that need to share employee information between facilities in the United States and foreign countries, such as members of the European Union, should be prepared to deal with the challenges those foreign countries present to the flow of employee information they are accustomed to in the United States.[23]

B. Federal Law

The federal government has yet to pass a broad-based data privacy and security statute. Instead, the federal approach has been to address specific types of information, in some cases on an industry-by-industry basis.[24] The touted privacy and security regulations under the Health Insurance Portability and Accountability Act of 1996[25] ("HIPAA") provided one of the first sets of comprehensive health data privacy and security safeguards issued by a federal agency.[26] However, the regulations generally apply only to *certain* types of health information, maintained by *certain* "covered entities"–health plans, health care providers, and health care clearinghouses, not employers.[27]

Other federal laws directed at enhancing privacy and security of personal information include the Gramm-Leach-Bliley Act of 1999[28]

21. *See* LUCAS BERGKAMP, EUROPEAN COMMUNITY LAW FOR THE NEW ECONOMY 118 (2003).

22. *Europe Clamps Down on Data Protection Violations: U.S. Multinational Fined for Cross-Border Data Transfer*, CLIENT ALERT (Thelen Reid Brown Raysman & Steiner LLP, New York, N.Y.), Aug. 2, 2007, at 1, *available at* http://www.thelen.com/resources/documents/PRIVACY_EUTyco_080207.pdf [hereinafter *Europe Clamps Down*]; Caslon Analytics, Privacy Guide: In the Workplace, http://www.caslon.com.au/privacyguide22.htm#law (last visited Aug. 28, 2008).

23. *See Europe Clamps Down*, *supra* note 22; Posting of Cecile Martin to Privacy Law Blog, http://privacylaw.proskauer.com/2007/12/articles/data-privacy-laws/focus-on-the-eu-and-france-can-us-employers-collect-sensitive-data-about-their-employees-resident-in-the-eu/ (Dec. 12, 2007, 6:40 AM).

24. *See* Harold C. Relyea, *Legislating Personal Privacy Protection: The Federal Response*, 27 J. ACAD. LIBRARIANSHIP 36, 44 (2001) (discussing the federal response on an area specific basis to privacy rights).

25. 45 C.F.R. §§ 160.101-164.534 (2007).

26. U.S. Department of Health and Human Services, National Institutes of Health, HIPAA Privacy Rule and Its Impacts on Research, http://privacyruleandresearch.nih.gov/ (last visited Sept. 28, 2008).

27. 45 C.F.R. § 160.103 (2007).

28. 15 U.S.C. §§ 6801-6809 (2000).

("GLB"), the Telephone Records and Privacy Protection Act of 2006[29] and the Veterans Benefits, Health Care, and Information Technology Act of 2006.[30] Consistent with the overall federal approach, these laws apply to specific industries and/or types of information. For example, GLB applies only to certain entities in the financial or insurance industries, and not to the personal information of employees as employees of those entities.[31] Where federal regulations apply to an employee's personal information, they too have been limited.[32] Examples include:

> Family and Medical Leave Act[33] – "Records and documents relating to medical certifications, recertifications or medical histories of employees or employees' family members, created for purposes of FMLA, shall be maintained as confidential medical records in separate files/records from the usual personnel files";[34]
>
> Americans with Disabilities Act[35] – An employee's medical records generally must be kept confidential and, for example, may not be kept as part of the employee's personnel file;[36]
>
> Fair Credit Reporting Act[37] – Employers who obtain consumer information provided by a third-party consumer reporting agency who conducts a background check subject to the Fair Credit Reporting Act must properly dispose of such information by taking "reasonable measures" to protect against the unauthorized access and possession of the information.[38]

A number of bills was expected to be taken up in the 110th

29. 18 U.S.C.A. § 1039 (Supp. 2008) (criminalizing and providing civil remedies for the practice known as "pretexting," or obtaining phone records under false pretenses).

30. Pub. L. No. 109-461, 120 Stat. 3403 (codified as amended in scattered sections of 38 U.S.C.) (requiring the VA to include data security provisions in all service-provider contracts, such as requiring that the contractor notify the VA of any breach).

31. *Cf.* Relyea, *supra* note 24, at 44 (discussing the scope of GLB).

32. *See infra* notes 33-38 and accompanying text.

33. 29 U.S.C. §§ 2601-2654 (2000).

34. 29 C.F.R. § 825.500(g) (2006).

35. 42 U.S.C. §§ 12101-12213 (2000).

36. 29 C.F.R. § 1630.14(c)(1) (2007).

37. 15 U.S.C. § 1681-1681x (2006).

38. 16 C.F.R. § 682.3(a) (2007); *New Requirement for Employers Who Use Third Parties to Conduct Background Checks*, CLIENT ALERT (Womble Carlyle Sandridge & Rice, PLLC., Winston-Salem, N.C.), June 2005, at 1, *available at* http://www.wcsr.com/downloads/pdfs/le060705.pdf.

Congress, a least one of which would have required data security programs to protect personal information.[39] The Personal Privacy and Data Security Act,[40] for example, introduced by Senators Patrick Leahy (D-VT) and Arlen Specter (R-PA) on February 6, 2007, is designed to prevent data breaches and mitigate their effects should they occur.[41] Senators Leahy and Specter's proposal would achieve this goal through two key provisions: (i) require certain businesses to establish data privacy and security programs[42] and (ii) provide a national standard for notifying U.S. persons when there has been an unauthorized breach of their personal information.[43] Unfortunately, at the time of this writing, none of these bills made it to the President's desk.[44]

C. State Law

States have been aggressive in their enactments to protect the personal information of their residents.[45] Key components of the "cocktail" approach employed by the states to prevent identity theft include (i) specific protections for Social Security Numbers, (ii) notification of unauthorized breaches of personal information, (iii) affirmative obligations to safeguard personal information, and (iv) the proper destruction of records containing personal information that are no longer needed.[46] Each of these is discussed below.

States that have enacted one or more of these measures generally have applied them to all entities doing business in the states.[47] In addition, the personal information protected generally is defined as the "first name or first initial and last name [of an individual], in combination with [the individual's] . . . (i) Social security number; (ii) Driver's license number or state identification card number; (iii)

39. S. 495, 110th Cong. § 301 (2007); *see also* Notification of Risk to Personal Data Act of 2007, S. 239, 110th Cong. § 1 (2007) (requiring disclosure of any breach of information relating to a person's identity by both federal agencies and individuals participating in interstate commerce).

40. S. 495, 110th Cong. § 1 (2007).

41. S. 495 § 2.

42. S. 495 § 302.

43. S. 495 § 311.

44. *See* GovTrack.us, S. 239: Notification of Risk to Personal Data Act of 2007, http://www.govtrack.us/congress/bill.xpd?bill=s110-239 (last visited Sept. 28, 2008); GovTrack.us, S. 495: Personal Data Privacy and Security Act of 2007, http://www.govtrack.us/congress/bill.xpd?bill=s110-495 (last visited Sept. 28, 2008).

45. *See supra* note 2 and accompanying text.

46. *See* discussion *infra* pp. 107-13.

47. *See, e.g.*, CAL. CIV. CODE § 1798.82(a) (West Supp. 2008); N.J. STAT. ANN. § 56:8-163 to -164 (West Supp. 2007); N.Y. GEN. BUS. LAW § 899-aa(3) (McKinney Supp. 2008).

Account number or 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."[48] Given the broad application of these statutes, the compliance effort for any organization will be significant, particularly for business that operate in many states, have high turnover, and/or maintain or process personal information on behalf of others.

1. Social Security Number Protections

Many states provide protections for Social Security Numbers ("SSNs") in certain specific situations, such as the use of SSNs in state property records and by insurance companies.[49] We discuss here the emergence of generally applicable state statutes which more than one-half of the states have enacted to limit the collection, use, and disclosure of SSNs.[50] These laws generally apply to all businesses operating in the state.[51]

Most of the state SSN statutes referenced above generally prohibit, with some exceptions, certain uses and disclosures of SSNs, such as (i) posting in public or showing to the public an individual's SSN; (ii) printing the SSN of an individual on any product and service access cards; (iii) requiring an individual to send his or her SSN via the

48. OHIO REV. CODE ANN. § 1349.19(A)(7)(a) (West Supp. 2007); *see also* CAL. CIV. CODE § 1798.82(e) (West Supp. 2008) (defining "personal information" in similar or virtually identical language); N.J. STAT. ANN. § 56:8-161 (West Supp. 2007) (same); N.Y. GEN. BUS. § 899-aa(1)(b) (McKinney Supp. 2008) (same).

49. *See, e.g.*, CAL. CIV. CODE § 1798.85(d)(1) (West Supp. 2008); 815 ILL. COMP. STAT. ANN. § 505/2QQ (West Supp. 2007); MICH. COMP. LAWS ANN. § 445.83(1)(g)(iv)(B) (West Supp. 2007); *see also* Joyita R. Basu, *State Statutes Restricting or Prohibiting the Use of Social Security Numbers*, PRIVACY BULL. (Morrison & Foerster, New York, N.Y.) Nov. 8, 2007, http://www.mofo.com/news/updates/bulletins/13038.html (mentioning that some state statutes pertaining to social security numbers specifically address insurance companies) (last visited Sept. 28, 2008).

50. *See, e.g.*, ARIZ. REV. STAT. ANN. § 44-1373 (Supp. 2007); ARK. CODE ANN. § 4-86-107 (Supp. 2007); CAL. CIV. CODE § 1798.85-.86 (West Supp. 2008); COLO. REV. STAT. ANN. § 6-1-715 (West Supp. 2007); CONN. GEN. STAT. ANN. § 42-470 (West Supp. 2007); GA. CODE ANN. §10-1-393.8 (Supp. 2007); 815 ILL. COMP. STAT. ANN. §§ 505/2QQ, /2RR (West Supp. 2007); MD. CODE ANN., COM. LAW § 14-3402 (West Supp. 2007); MICH. COMP. LAWS ANN. § 445.83 (West Supp. 2007); MINN. STAT. ANN. § 325E.59 (West Supp. 2008); MO. ANN. STAT. § 407.1355 (West Supp. 2008); N.J. STAT. ANN. § 56:8-164 (West Supp. 2007); N.Y. GEN. BUS. LAW § 399-dd (McKinney Supp. 2008); N.C. GEN. STAT. § 75-62 (2007); OKLA. STAT. ANN. tit. 40, § 173.1 (West Supp. 2008); R.I. GEN. LAWS § 6-48-8 (Supp. 2007); TEX. BUS. & COM. CODE ANN. § 35.58 (Vernon Supp. 2007); VT. STAT. ANN. tit. 9, § 2440 (West 2007); VA. CODE. ANN. § 59.1-443.2 (2006).

51. Basu, *supra* note 49.

Internet, except where a secure connection is used or where the SSN being transmitted has been encrypted; (iv) insisting an individual provide his or her SSN in order to enter a web site on the Internet, except where access also involves the utilization of a password, unique personal identification number, or some other verification tool; and (v) printing a person's SSN on anything being sent to that individual by mail, unless there is an applicable state or federal law either requires or allows the SSN to be printed on the mailed item.[52] States such as California, Connecticut, New York and Michigan have additional requirements, some of which are briefly discussed below.[53]

Beginning January 1, 2008, California employers are prohibited from showing more than the last four digits of an employee's SSN on the detachable portion of the check, draft or voucher paying the employee's wages.[54] In New York, also beginning January 1, 2008, businesses possessing SSNs must implement "safeguards necessary or appropriate to preclude unauthorized access to . . . and protect the confidentiality of" SSNs.[55] In Michigan, businesses that obtain SSNs in the ordinary course of business must develop a privacy policy that protects SSN confidentiality, limits improper uses and disclosure of SSNs, illustrates the correct disposal method for documents with SSNs, and sets forth penalties for policy violations.[56] Likewise, in Connecticut, any business in the state that collects SSNs must publish or publically display a policy concerning the confidentiality, unlawful disclosure, or limited access to SSNs.[57]

For businesses, particularly when wearing their employer hat, SSNs continue to be in widespread use—identifying and tracking employees for a variety of purposes, including benefit plan enrollment, running background checks, federal and state tax reporting, and so on.[58] Best practice dictates that businesses and practitioners simply limit the use of SSNs to the extent possible, such as by creating alternative identifiers for employees or eliminating SSNs from leave request and application

52. *See* statutes cited *supra* note 50.

53. *See infra* notes 54-56 and accompanying text.

54. CAL. LAB. CODE § 226(a)(7) (West Supp. 2008).

55. N.Y. GEN. BUS. LAW § 399-dd(4) (McKinney Supp. 2008). New York recently added requirements to protect SSN protections specifically on employers. S.B. S08376A, 2008 Leg., Reg. Sess. § 6 (N.Y. 2008) (to be codified at N.Y. LAB. LAW § 203-d).

56. MICH. COMP. LAWS ANN. § 445.84 (West Supp. 2007).

57. 2008 Conn. Acts No. 08-167 (Reg. Sess.).

58. Danielle Keats Citron, *Reservoirs of Danger: The Evolution of Public and Private Law at the Dawn of the Information Age*, 80 S. CAL. L. REV. 241, 248 (2007).

forms.[59]

2. Affirmative Obligations to Protect Personal Information

In an increasing number of states, it is not enough to protect SSNs. Instead, businesses in these states need to take a more proactive and comprehensive approach to safeguarding personal information.

For example, in California, "[a] business that owns or licenses personal information about a California resident [must] implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure."[60] Similar requirements were enacted in other states, such as Arkansas, Connecticut, Maryland, Massachusetts, Nevada, North Carolina, Oregon, Rhode Island, Texas, and Utah.[61]

Some of these states provide more specific requirements. For example, in Nevada, a contract involving the disclosure of a resident's personal information "must include a provision requiring the person to whom the information is disclosed to implement" safeguards to protect that information.[62] Oregon's Consumer Identity Theft Protection Act,[63] however, lays out more specific requirements, with some relief for small businesses (those businesses with 100 employees or less).[64] Key among those is the requirement to implement an "information security and

59. *See* Patrick Gavin, *Legal Edge: Respecting Employee Privacy*, KANSAS CITY SMALL BUS. MONTHLY (Nov. 2007), http://www.kcsmallbiz.com/november-2007/legal-edge-respecting-employee-privacy-2.html (last visited Sept. 28, 2008).

60. CAL. CIV. CODE § 1798.81.5 (West Supp. 2008).

61. ARK. CODE ANN. § 4-110-104(b) (Supp. 2007); 2008 Conn. Acts No. 08-167 (Reg. Sess.); MD. CODE ANN., COM. LAW § 14-3503(a) (West Supp. 2007); NEV. REV. STAT. ANN. § 603A.210 (West Supp. 2007); N.C. GEN. STAT. § 75-64(a) (2007); OR. REV. STAT. ANN. § 646A.622(1) (West Supp. 2008); R.I. GEN. LAWS § 11-49.2-2(2) (Supp. 2007); TEX. BUS. & COM. CODE ANN. § 48.102(a) (Vernon Supp. 2007); UTAH CODE ANN. § 13-44-201(1)(a) (Supp. 2007); H.B. 4144, 185th Gen. Ct., Reg. Sess., ch. 93H, § 2(a) (Mass. 2007) (enacted) (pursuant to which the department of consumer affairs and business regulation adopted regulations requiring business entities among others to safeguard any personal information about residents that the covered entity owns or licenses).

62. NEV. REV. STAT. ANN. § 603A.210(2) (West Supp. 2007).

63. OR. REV. STAT. ANN. §§ 646A.600 to .628 (West Supp. 2008).

64. OR. REV. STAT. ANN. § 646A.622(4) (West Supp. 2008). A "small business" is defined at section 285B.123(3) of the Oregon Revised Statutes. Small businesses in Oregon need not establish a full-blown information security programs as described in the text. *Id.* Instead, small businesses will be deemed to comply where their "information security and disposal program contains administrative, technical and physical safeguards and disposal measures appropriate to the size and complexity of the business, and the sensitivity of the personal information collected." *Id.*

disposal program" that contains "administrative, technical and physical safeguards."[65]

Under the Oregon Act, administrative safeguards include:

> (i) Designat[ing] one or more employees to coordinate the security program;
>
> (ii) Identify[ing] reasonably foreseeable internal and external risks;
>
> (iii) Assess[ing] the sufficiency of [data] safeguards . . . ;
>
> (iv) Train[ing] and manag[ing] employees in the security program practices and procedures;
>
> (v) Select[ing] service providers capable of maintaining appropriate safeguards, and require[ing] those safeguards by contract; and
>
> (vi) Adjust[ing] the security program in light of business changes or new circumstances.[66]

The Act also lists examples of technical safeguards, such as requiring the designated employee coordinator to assess risk in electronic networks, software and storage, and performing regular checks of the success of key controls and procedures.[67] Examples of physical safeguards under the Act include those that would require businesses to: assess the risks of the storage and disposal of personal information; identify intrusions, protect against and fix such breaches; shield "against unauthorized access to or use of personal information during . . . the collection, transportation and destruction or disposal of such information"; and "dispose[] of personal information after it is no longer needed for business purposes or as required by . . . law by burning, pulverizing, shredding or modifying a physical [or electronic record] . . . so that the information cannot be read or reconstructed."[68]

To date, the most comprehensive broad-based protections of

65. *Id.*
66. *Id.* § 646A.622(2)(d)(A).
67. *Id.* § 646A.622(2)(d)(B).
68. *Id.* § 646A.622(2)(d)(C).

personal data at the state level exist in regulations issued by The Massachusetts Office of Consumer Affairs and Business Regulation.[69] Effective January 1, 2009, these regulations establish minimum standards for protecting and storing personal information about Massachusetts residents contained in paper or electronic format.[70] The rules apply to any businesses or individuals that own, license, store or maintain personal information about a Massachusetts resident, potentially having extra-territorial effect, covering businesses or individuals possessing the personal information of Massachusetts residents but with no presence in Massachusetts.[71]

Under the regulation, covered persons and entities must "develop, implement, maintain and monitor" a written, comprehensive information security program applicable to any records containing personal information, which includes administrative, technical, and physical safeguards.[72] Without intending to provide an exhaustive list of safeguards, the regulations list safeguards that must be a part of any comprehensive information security program.[73] Examples include:

> Designate one or more employees to maintain the program;[74]
>
> Conduct risk assessments to gauge risks to the security, confidentiality, and/or integrity of any electronic, paper or other records containing personal information;[75]
>
> Before providing a vendor access to personal information, obtain a written certification that the vendor has a compliant comprehensive information security program that complies with the Massachusetts regulations;[76]
>
> Impose reasonable restrictions on physical access to records containing personal information, including a written procedure that sets forth the

69. MASS. CODE REGS.§ 17.00 (2008).
70. *Id.*
71. *Id.* § 17.01(1).
72. *Id.* § 17.03(1).
73. *Id.* § 17.03(2)(d).
74. *Id.* § 17.03(2)(d)(1).
75. *Id.* § 17.03(2)(d)(2).
76. *Id.* § 17.03(2)(d)(6).

> manner in which physical access to such records is restricted;[77]
>
> Document steps taken to respond to a security breach and any changes in safeguards resulting from a review of the breach incident.[78]

The regulations provide further safeguards that specifically apply to electronically stored or transmitted personal information. These include establishing and maintaining a security system covering its computers, including any wireless systems.[79] To the extent feasible, records containing personal information that is transmitted across public networks and wirelessly must be encrypted.[80] Perhaps more significant is that all personal information stored on laptops and portable devices must be encrypted.[81]

When evaluating whether a particular program includes reasonable and appropriate safeguards, similar to other jurisdictions, the Massachusetts data security regulations permit the person or entity to take into account size, scope and type of business, resources available, amount of stored data, and need for security and confidentiality of both consumer and employee information.[82]

The emergence of these state mandates, on the heels of HIPAA and GLB, and fueled by the continued rapid advancement and increasing use of technology, suggest a trend that is sure to become a fact of life for businesses operating anywhere in the United States. Accordingly, businesses need to be guided now to take appropriate steps to protect the personal information they maintain throughout their organizations. It is no longer sufficient to be concerned only about SSNs, or information protected by HIPAA or GLB.

3. Data Breach Notification

While the federal government has yet to provide a national standard for breach notification, over 40 states have enacted breach notification laws.[83] The essence of these statutes is to require businesses to notify

77. *Id.* § 17.03(2)(d)(9).
78. *Id.* § 17.03(2)(d)(11).
79. *Id.* § 17.04.
80. *Id.* § 17.04(3).
81. *Id.* § 17.04(5).
82. *Id.* § 17.03(2).
83. *See* ARIZ. REV. STAT. ANN. § 44-7501 (Supp. 2007); ARK. CODE ANN. § 4-110-105 (Supp. 2007); CAL. CIV. CODE § 1798.82 (West Supp. 2008); COLO. REV. STAT. ANN. § 6-1-716 (West Supp. 2007); CONN. GEN. STAT. ANN. § 36a-701b (West Supp. 2007); DEL. CODE ANN. tit. 6,

affected individuals and/or certain governmental entities and credit reporting agencies when there has been an unauthorized breach of personal information maintained by the business.[84] Even businesses with comprehensive data protection safeguards experience data breaches.[85] The point of these notifications statutes, however, is to warn affected individuals and give them more time to protect themselves and mitigate any harm that might be caused by the breach.[86]

The key issues for businesses and practitioners in this area are to know which laws apply and be prepared to provide notice quickly. For businesses with large numbers of employees/customers and operations in more than one state, this becomes increasingly difficult. These key issues and others are discussed below.

i. Who is Covered?

Most state breach notification laws apply to any company doing business in that state if the company "owns or licenses" information protected by the applicable state law.[87] There generally are no

§§ 12B-101 to -104 (West 2006); D.C. CODE §§ 28-3851 to -3853 (Supp. 2007); FLA. STAT. ANN. § 817.5681 (West 2005); GA. CODE ANN. §§10-1-910 to -912 (Supp. 2007); HAW. REV. STAT. §§ 487N-1 to -4 (Supp. 2007); IDAHO CODE ANN. §§ 28-51-104 to -107 (2005 & Supp. 2008); 815 ILL. COMP. STAT. ANN. 530/1, /5, /10, /12 (West Supp. 2007); IND. CODE ANN. §§ 24-4.9-1-1 to -5-1 (West Supp. 2008); KAN. STAT. ANN. §§ 50-701 to -722 (1994); LA. REV. STAT. ANN. §§ 51:3071 to :3077 (Supp. 2008); ME. REV. STAT. ANN. tit. 10, §§ 1346 to 1350-A (Supp. 2007); MD. CODE ANN., COM. LAW §§ 14-3501 to -3508 (West Supp. 2007); H.B. 4144, 185th Gen. Ct., Reg. Sess., ch. 93H, §§ 1-6 (Mass. 2007) (to be codified at MASS. GEN. LAWS §§ 93H-1 to -6); MICH. COMP. LAWS ANN. § 445.72 (West Supp. 2007); MINN. STAT. ANN. § 325E.61 (West Supp. 2008); MONT. CODE. ANN. § 30-14-1704 (2007); NEB. REV. STAT. ANN. §§ 87-801 to -807 (LexisNexis 2007); NEV. REV. STAT. ANN. §§ 603A.010 to .040 (West Supp. 2007); N.H. REV. STAT. ANN. §§ 359-C:19 to :21 (Supp. 2007); N.J. STAT. ANN. §§ 56:8-161 to -166 (West Supp. 2007); N.Y. GEN. BUS. LAW § 899-aa (McKinney Supp. 2008); N.C. GEN. STAT. §§ 75-65 (2007); N.D. CENT. CODE §§ 51-30-01 to -07 (2007); OHIO REV. CODE ANN. § 1349.19 (West Supp. 2007); OKLA. STAT. ANN. tit. 74, § 3113.1 (West Supp. 2008); OR. REV. STAT. ANN. § 646A.604 (West Supp. 2008); 73 PA. CONS. STAT. ANN. §§ 2301-2308 (West Supp. 2007); R.I. GEN. LAWS §§ 11-49.2-1 to -7 (Supp. 2007); TENN. CODE ANN. § 47-18-2107 (2008); TEX. BUS. & COM. CODE ANN. §§ 48.103 (Vernon Supp. 2007); UTAH CODE ANN. § 13-44-202 (Supp. 2007); VT. STAT. ANN. tit. 9, §§ 2435 (West 2007); WASH. REV. CODE ANN. § 19.255.010 (West 2007); W. VA. CODE §§ 46A-2-101 to -105 (West 2008); WIS. STAT. ANN. § 895.507 (West 2006); WYO. STAT. ANN. § 40-12-502 (2007); H.B. 65, 2008 Leg., Reg. Sess. § 4 (Ala. 2008) (to be codified at ALASKA STAT. § 45.48.101 to .995); S.B. 2308, 2008 Leg., Reg. Sess. § 1 (Iowa 2008) (to be codified at IOWA CODE § 715C.1); H.R. A190, Gen. Assem., 117th Sess. §§1-12 (S.C. 2008). *See also* P.R. LAWS ANN. tit. 10, § 4051 (Supp. 2006); V.I. CODE ANN. tit. 14, § 2208 (2006).

84. *See, e.g.*, ARIZ. REV. STAT. ANN. § 44-7501(A) (Supp. 2007).

85. *See, e.g.*, Jewellap, *supra* note 12.

86. *See, e.g.*, MONT. CODE ANN. § 30-14-1704(1) (2007).

87. *See, e.g.*, ARIZ. REV. STAT. ANN. § 44-7501(A) (Supp. 2007); CAL. CIV. CODE §

exceptions for small employers. In some states, entities required to notify individuals need not own or license the information, but need only maintain it.[88] In Georgia and Maine, the laws apply only to those entities that are *in the business of* collecting, maintaining, transferring, and evaluating, etc. personal information *for monetary fees or dues*.[89] In these states, for example, private companies in their capacity as employers likely would not be affected.

It is important, therefore, for businesses and practitioners to understand the different capacities in which a business may maintain personal information and how the law might apply. For example, a company that provides data storage services for other companies likely would be subject to these statutes but generally would be required to notify only the company that owns or licenses the information, not the affected individuals.[90]

Some states have expressly excluded or deemed to be in compliance certain entities that have similar obligations under other statutes, regulations, or programs such as:

The GLB;[91]

The Federal Interagency Guidance Response Programs for Unauthorized Access to Consumer Information and Consumer

1798.82(a) (West Supp. 2008).

88. *See, e.g.*, CONN. GEN. STAT. ANN. § 36a-701b(b) (West Supp. 2007); FLA. STAT. ANN. § 817.5681(1)(a) (West 2005); N.J. STAT. ANN. § 56:8-163(a) (West Supp. 2007).

89. GA. CODE ANN. § 10-1-911(3) (Supp. 2007); ME. REV. STAT. ANN. tit. 10, § 1347(3) (Supp. 2007) (defining "information broker").

90. *See, e.g.*, CONN. GEN. STAT. ANN § 36a-701b(c) (West Supp. 2007); FLA. STAT. ANN. § 817.5681(2)(a) (West 2005); 815 ILL. COMP. STAT. ANN. 530/10(b) (West Supp. 2007); MINN. STAT. ANN. § 325E.61(1)(b) (West Supp. 2008); N.J. STAT. ANN. § 56:8-163(b) (West Supp. 2007); N.Y. GEN. BUS. LAW § 899-aa(3) (McKinney Supp. 2008); 73 PA. CONS. STAT. ANN. § 2303(a) (West Supp. 2007); TEX. BUS. & COM. CODE ANN. § 48.103(c) (Vernon 2008). In some states, such as Arizona and Florida, the owners and non-owners of the information may enter into an agreement allocating the responsibility to provide the notice. ARIZ. REV. STAT. ANN. § 44-7501(B) (Supp. 2007); FLA. STAT. ANN. § 817.5681(2)(a) (West 2005). Note also that Florida law requires non-owners to notify owners of the breach within 10 days after a determination of a breach. FLA. STAT. ANN. § 817.5681(2)(b) (West 2005).

91. *See, e.g.*, ARIZ. REV. STAT. ANN. § 44-7501(J)(1) (Supp. 2007); COLO. REV. STAT. ANN. § 6-1-716(2)(d) (West Supp. 2007); CONN. GEN. STAT. ANN. § 36a-701b(f) (West Supp. 2007); MINN. STAT. ANN. 325E.61(4) (West Supp. 2008); NEV. REV. STAT. ANN. § 603A.220(5)(b) (West Supp. 2007); N.H. REV. STAT. ANN. § 359-C:20(VI)(b) (Supp. 2007); TENN. CODE ANN. § 47-18-2107(i) (2008); TEX. BUS. & COM. CODE ANN. § 48.101(c)(1) (Vernon 2008); UTAH CODE ANN. § 13-42-201(3) (Supp. 2007).

Notice;[92]

The privacy and security regulations issued under HIPAA.[93] Practitioners should note that HIPAA only applies to certain "covered entities," at the exclusion of all others.[94] Thus, while a health plan that an employer sponsors typically is subject to the HIPAA requirements, the employer is not. Accordingly, it follows that the exemption under these state laws would apply to covered entities under HIPAA, not companies in their capacity as employers, and/or;

Rules, regulations, procedures, or other guidance established by the entity's primary or functional federal regulator.[95]

ii. What Information is Protected?

Most state breach notification laws extend to all residents and protect "personal information."[96] As noted above, personal information typically is defined as the first name or first initial and last name of an individual, in combination with the individual's (i) social security number; (ii) driver's license number; (iii) state identification number; (iv) financial account, debit or credit card number in combination with any required security code, access code, or password that would permit access to an individual's account.[97] In most cases, this includes only computerized personal information, although some state breach notification laws also apply to personal information in hardcopy, as

92. *See, e.g.*, LA. REV. STAT. ANN. § 51:3076 (2003); N.C. GEN. STAT. § 75-65(h) (2007); 73 PA. CONS. STAT. ANN. § 2307(b)(1) (West Supp. 2007).

93. *See, e.g.*, ARIZ. REV. STAT. ANN. § 44-7501(J)(2) (Supp. 2007); MINN. STAT. ANN. § 325E.61(4) (West Supp. 2008); OHIO REV. CODE ANN. § 1349.19(F)(2) (West Supp. 2008); R.I. GEN. LAWS § 11-49.2-7 (Supp. 2007).

94. 45 C.F.R. § 160.103 (defining "covered entity").

95. *See, e.g.*, ARIZ. REV. STAT. ANN. § 44-7501(F) (Supp. 2007); ARK. CODE. ANN. § 4-110-106 (Supp. 2007); COLO. REV. STAT. ANN. § 6-1-716(3)(b) (West Supp. 2007); DEL. CODE ANN tit. 6, § 12B-103(b) (West 2006); FLA. STAT. ANN. § 817.5681(9)(b) (West 2005); IDAHO CODE ANN. § 28-51-106(2) (Supp. 2007); N.H. REV. STAT. ANN. § 359-C:20(V) (Supp. 2007); N.D. CENT. CODE § 51-30-06 (Supp. 2007); OHIO REV. CODE ANN. § 1349.19(F)(1) (West Supp. 2006); 73 PA. CONS. STAT. ANN. § 2307(b)(2) (West Supp. 2007); R.I. GEN. LAWS § 11-49.2-7 (Supp. 2007).

96. *See, e.g.*, CAL. CIV. CODE § 1798.81.5(a) (West Supp. 2007); N.J. STAT. ANN. § 56:8-163(a) (West Supp. 2007).

97. *See, e.g.*, CAL. CIV. CODE § 1798.82(e) (West Supp. 2007); N.J. STAT. ANN. § 56:8-161 (West Supp. 2007); N.Y. GEN. BUS. LAW § 899-aa(1)(b) (McKinney Supp. 2008); OHIO REV. CODE ANN. § 1349.19(A)(7) (West Supp. 2007).

opposed to electronic, format.[98] Thus, in most states, a company that is not otherwise exempt will have to comply with respect to the personal information it collects, handles, maintains, etc. in the course of its business, as well as the personal information it collects, handles, maintains, etc. as an employer, or in any other non-exempt status.

A few states cast a wider net on the types of protected information.[99] In Arkansas, notification is required if medical information is breached.[100] California recently amended its statute to do the same.[101] In North Dakota, for example, "personal [identifying] information" also includes information such as the identification number assigned to an individual by his or her employer, the maiden name of the individual's mother, and the individual's digital signature.[102]

Almost all states provide what is in effect a safe harbor for encrypted information; that is, if otherwise protected personal information is subjected to an unauthorized breach, but the information is encrypted, notification is not required.[103] However, where the breach also gives access to the keys for unencrypting the encrypted information, the information will be treated as if it was not encrypted and notification will be required.[104] Thus, one way to limit exposure under these statutes is to encrypt all of the information that is subject to these laws; provided, however, that the key to the encryption is not also accessed. As a practical matter, however, encryption may not be available to all businesses.

iii. When is the notification requirement triggered?

Not all breaches are the same; that is, some may not require notice

98. *See, e.g.*, IND. CODE ANN. § 24-4.9-2-2 (West 2006); H.B. 4144, 185th Gen. Ct., Reg. Sess., ch. 93H, § 1(a) (Mass. 2007) (enacted); N.C. GEN. STAT. §§ 75-61(12), (14) (2007); WIS. STAT. § 895.507(2)(a) (West 2006).

99. *See, e.g.*, ARK. CODE ANN. § 4-110-103(7)(D) (Supp. 2007); Assemb. B. No. 1298, 2007-2008 Leg. Sess., ch. 699, § 4(e)(4), (5) (Cal. 2007) (enacted); N.C. GEN. STAT. § 75-61(10) (2007); N.D. CENT. CODE § 51-30-01(2)(a) (2007); UTAH CODE ANN. § 13-44-102(3) (Supp. 2007).

100. ARK. CODE ANN. § 4-110-103(7)(D) (Supp. 2007).

101. Assemb. B. No. 1298, 2007-2008 Leg. Sess., ch. 699, § 4(e)(4) (Cal. 2007) (enacted).

102. N.D. CENT. CODE § 51-30-01(2)(a) (2008).

103. *See, e.g.*, ARIZ. REV. STAT. ANN. § 44-7501(A) (Supp. 2007); CAL. CIV. CODE § 1798.82(e) (West Supp. 2008); COLO. REV. STAT. ANN. § 6-1-716(1)(a) (West Supp. 2007); FLA. STAT. ANN § 817.5681(1)(a) (West 2005); N.D. CENT. CODE § 51-30-01(1) (2007). *But see* UTAH CODE ANN. § 13-44-102(1) (Supp. 2007) (omitting the term encryption from the definition of "[b]reach of system security").

104. *See, e.g.*, N.H. REV. STAT. ANN. § 359-C:19(II) (Supp. 2007); N.Y. GEN. BUS. LAW § 899-aa(1)(b) (McKinney Supp. 2008); 73 PA. CONS. STAT. ANN. § 2303(b) (West Supp. 2007).

of a breach be provided to affected individuals. Some states require notice to affected parties only if the company determines, after an investigation, that the breach will likely result in harm to the individual or the misuse of the personal information.[105] For example, in Florida, New Jersey, and Oregon, if an entity, after an appropriate investigation, determines that the breach is unlikely to result in harm to the individuals whose information was accessed then the entity need not notify the affected individuals, instead the entity determination must be documented and retained for five years.[106] Of course, other states require a notice regardless of whether there is a likelihood that harm will result.[107]

iv. Who must be notified?

In general, breach notification statutes require notice be provided to the affected residents of the state.[108] In some state, such as California, notice to residents is all that is in fact required by the statute.[109] However, in other states a security breach triggers additional notice requirements. For example, in New York, the statute requires that notice not only be provided to the affected individual, but it also must be provided to the state Attorney General, the Consumer Protection Board, and the state Office of Cyber Security and Critical Infrastructure Coordination.[110] Other states predicate additional reporting requirements on the number of individuals affected by the breach. Specifically, where the number of affected residents exceeds a certain amount, often 1,000, in a single breach, many breach notification laws require the covered business to notify consumer reporting agencies, and

105. *See, e.g.*, COLO. REV. STAT. ANN. § 6-1-716(2)(a) (West Supp. 2007); LA. REV. STAT. ANN. § 51:3074(G) (2003); N.C. GEN. STAT. § 75-61(14) (2007); 73 PA. CONS. STAT. ANN. § 2302 (West Supp. 2007); WASH. REV. CODE ANN. § 19.255.010(10)(d) (West 2007).

106. FLA. STAT. ANN. § 817.5681(10)(a) (West 2005); N.J. STAT. ANN. § 56:8-163(a) (West Supp. 2007); OR. REV. STAT. ANN. § 646A.604(7) (West Supp. 2008).

107. *See, e.g.*, CAL. CIV. CODE § 1798.82(a) (West Supp. 2008); DEL. CODE ANN. tit. 6, § 12B-102(a) (West 2006); 815 ILL. COMP. STAT. ANN. 530/10(a) (West Supp. 2007); ME. REV. STAT. ANN. tit. 10, § 1348(1) (Supp. 2007); N.Y. GEN. BUS. LAW §899-aa(2) (McKinney Supp. 2008); TEX. BUS. & COM. CODE ANN. § 48.103(b) (Vernon Supp. 2007).

108. *See, e.g.*, CAL. CIV. CODE § 1798.82(a) (West Supp. 2008); 815 ILL. COMP. STAT. ANN. 530/10(a) (West Supp. 2007); ME. REV. STAT. ANN. tit. 10, § 1348(1) (Supp. 2007); N.Y. GEN. BUS. LAW § 899-aa(2) (McKinney Supp. 2008); TEX. BUS. & COM. CODE ANN. § 48.103(b) (Vernon Supp. 2007).

109. CAL. CIV. CODE § 1798.82(a) (West Supp. 2008).

110. N.Y. GEN. BUS. LAW § 899-aa(8)(a) (McKinney Supp. 2008).

in some cases certain state agencies.[111]

v. What are the specific notice requirements?

Notice requirements with regard to form, content, timing, and substitute notice vary from state to state. Some states, for example, permit notification by either regular or electronic mail[112] and others, by telephone.[113] In addition, virtually all states permit a substitute notice to be used in place of notifying each affected person individually under circumstances where providing notice is a significant burden.[114] For example, a substitute notice is permitted in California, if: (i) the cost to provide the notice exceeds $250,000, (ii) more than 500,000 individuals are affected, or (iii) the company does not have up to date contact information.[115]

Some states specify the content of the notice. For example, Hawaii requires that the notice be "clear and conspicuous" and include the

111. *See, e.g.*, COLO. REV. STAT. ANN. § 6-1-716(2)(d) (West Supp. 2007) (requires notification to consumer reporting agencies where breach affects 1,000 or more individuals); FLA. STAT. ANN. § 817.5681(12) (West 2005) (requires notification to consumer reporting agencies where breach affects 1,000 or more individuals); MINN. STAT. ANN. § 325E.61(2) (West Supp. 2008) (requires notification to consumer reporting agencies where breach affects 500 or more individuals); N.H. REV. STAT. ANN. § 359-C:20(VI)(a) (Supp. 2007) (requires notification to consumer reporting agencies where breach affects 1,000 or more individuals); N.Y. GEN. BUS. LAW § 899-aa(8)(b) (McKinney Supp. 2008) (requires notification to consumer reporting agencies where breach affects 5,000 or more individuals); N.C. GEN. STAT. § 75-65(f) (2007) (requires notification to consumer reporting agencies where breach affects 1,000 or more individuals); TEX. BUS. & COM. CODE ANN. § 48.103(h) (Vernon Supp. 2007) (requires notification to consumer reporting agencies where breach affects 10,000 or more individuals). For this purpose, the term "credit reporting agency" generally refers to those agencies that compile and maintain files on consumers on a nationwide basis as defined by 15 U.S.C. § 1681a(p) (2007).

112. *See, e.g.*, ARK. CODE ANN. § 4-110-105(e) (Supp. 2007); CAL. CIV. CODE § 1798.82(g) (West Supp. 2008); FLA. STAT. ANN. § 817.5681(6) (West 2005); 815 ILL. COMP. STAT. ANN. § 530/10(c) (West Supp. 2007); MINN. STAT. ANN. 325E.61(1)(g) (West Supp. 2008); N.J. STAT. ANN. § 56:8-163(d) (West Supp. 2007); TENN. CODE ANN. § 47-18-2107(e) (2008); TEX. BUS. & COM. CODE ANN. § 48.103(e) (Vernon Supp. 2007); WASH. REV. CODE ANN. § 19.255.010(7) (West 2007).

113. *See, e.g.*, ARIZ. REV. STAT. ANN. § 44-7501(D)(3) (Supp. 2007); COLO. REV. STAT. ANN. § 6-1-716(1)(c)(II) (West Supp. 2007); CONN. GEN. STAT. ANN. § 36a-701b(e) (West Supp. 2007); MONT. CODE. ANN. § 30-14-1704(5)(a)(iii) (2007); N.Y. GEN. BUS. LAW § 899-aa(5)(c) (McKinney Supp. 2008).

114. *See, e.g.*, ARIZ. REV. STAT. ANN. § 44-7501(D)(4) (Supp. 2007); ARK. CODE ANN. § 4-110-105(e)(3) (Supp. 2007); CAL. CIV. CODE § 1798.82(g)(3) (West Supp. 2008); CONN. GEN. STAT. ANN. § 36a-701b (e) (West Supp. 2007); FLA. STAT. ANN. § 817.5681(6)(c) (West 2005); 815 ILL. COMP. STAT. ANN. § 530/10(c)(3) (West Supp. 2007); MINN. STAT. ANN. § 325E.61(1)(g)(3) (West Supp. 2008).

115. CAL. CIV. CODE § 1798.82(g)(3) (West Supp. 2008).

following information:

> A description of the incident;
>
> The type of personal information subject to the breach;
>
> The actions taken by the company to protect the information;
>
> A telephone number the individual can call for additional information, if one exists; and
>
> Advice to remain vigilant, review account statements, and monitor free credit reports.[116]

Practitioners need to be aware of these requirements to ensure notices to affected individuals convey the appropriate information and do not open the door to unnecessary claims.

The timing of these notices is critical; all states generally require that the notice must be provided as soon as possible and without unreasonable delay, usually taking into account any measures necessary to determine the scope of the breach and to restore protections to the system breached.[117] All states, other than Illinois, permit a delay in notification where it would hinder a criminal investigation.[118] Notwithstanding a criminal investigation, Florida, Ohio and Wisconsin, require notice of a breach within a reasonable amount of time, which should not to exceed forty-five days after its discovery.[119]

The importance of this timing issue is highlighted by the action of

116. HAW. REV. STAT. § 487N-2(d) (Supp. 2007). *See also*, N.H. REV. STAT. ANN.§ 359-C:20(IV) (Supp. 2007) (enumerating similar minimum notice requirements); N.C. GEN. STAT. § 75-65(d) (2007) (same).

117. *See, e.g.*, ARK. CODE ANN. § 4-110-105(a)(2) (Supp. 2007); CAL. CIV. CODE § 1798.82(a) (West Supp. 2008); FLA. STAT. ANN. § 817.5681(1)(a) (West 2005); MINN. STAT. ANN. 325E.61(1)(a) (West Supp. 2008); N.J. STAT. ANN. § 56:8-163(a) (West Supp. 2007).

118. *Compare, e.g.*, FLA. STAT. ANN. § 817.5681(1)(a) (West 2005) (requiring disclosure in a manner "consistent with the legitimate needs of law enforcement"), MINN. STAT. ANN. 325E.61(1)(a) (West Supp. 2008) (same), *and* N.J. STAT. ANN. § 56:8-163(a) (West Supp. 2007) (same), *with* 815 ILL. COMP. STAT. ANN. § 530/10(a) (West Supp. 2007) (requiring disclosure in a manner "consistent with any measures necessary to determine the scope of the breach and restore the reasonable integrity, security, and confidentiality of the data system").

119. FLA. STAT. ANN. § 817.5681(1)(a) (West 2005); OHIO REV. CODE ANN. § 1349.19(B)(2) (West Supp. 2006); WIS. STAT. ANN. § 895.507(3)(a) (West 2006).

Attorney General Cuomo in New York who announced the first settlement dated April 26, 2007, under New York's Information Security Breach and Notification Law related to the prompt notification requirement.[120] The case involved a Chicago-based claims management company which did not provide the required breach notice, including notice to approximately 540,000 New York consumers, for seven weeks.[121] Without admitting to any violation of law and cooperating fully with the Attorney General's investigation, the company agreed to implement precautionary procedures, comply with New York's notification law in the event of a security breach, and pay the Attorney General's office $60,000 for costs related to this investigation.[122] According to Attorney General Cuomo,

> This company had sufficient cause to believe that the private information contained in the missing computer had been acquired by a person without valid authorization. Had the sensitive personal information fallen into the hands of criminals with the intent of identity theft, there would have been ample time to victimize hundreds of thousands of consumers. The law requires prompt notice to prevent such disastrous results.[123]

vi. How are these statutes enforced?

There generally are two avenues for enforcement of breach notification statutes – private rights of action by individuals, and actions by the state Attorney General for relief, including civil penalties, damages, and/or injunctive relief.[124] Examples include:

Arizona – enforcement only by Attorney General who may bring an action to obtain actual damages for a willful and knowing violation and civil penalties not to exceed $10,000.[125]

Delaware – enforcement only by Attorney General, pursuant to Consumer Protection Division of the Department of Justice.[126]

---

120. Press Release, Office of the N.Y. State Att'y Gen. Andrew M. Cuomo, Cuomo Obtains First Agreement for Violation of Security Breach Notification Law (Apr. 26, 2007), *available at* http://www.oag.state.ny.us/media_center/2007/apr/apr26a_07.html.

121. *Id.*

122. *Id.*

123. *Id.*

124. *See infra* notes 125-132.

125. ARIZ. REV. STAT. ANN. § 44-7501(H) (West. Supp. 2007).

126. DEL. CODE ANN. tit. 6, § 12B-104 (West 2006).

California and Washington – aggrieved individuals have a private right of action.[127]

New Hampshire – residents of the state damaged by a flawed notification have a private right of action and may obtain "as much as 3 times" the amount of actual damages, plus reasonable attorney's fees.[128]

Florida – businesses that fail to timely provide notice are subject to significant administrative penalties based on the timing of the notification; penalties can be up to $50,000.[129]

Louisiana – a private right of action is permitted for actual damages.[130]

Nevada – the Attorney General or district attorney may bring an action against any person he/she reasonably believes has violated any provisions of the notification chapter.[131]

New York – the Attorney General may recover actual and consequential damages for residents affected by the failure to notify.[132]

Texas – the Attorney General can recover civil penalties of $2,000 to $50,000.[133]

Individuals affected by data breaches have attempted to recover through litigation. The good news for companies is that many of these cases have been unsuccessful.[134] In *Bodah v. Lakeville Motor Express, Inc.*,[135] employees filed a class-action lawsuit against their employer, following union complaints, alleging that the employer's decision to fax a list of their names and Social Security numbers to managers, for the purpose of tracking terminal accidents and injuries, amounted to a common law invasion of privacy.[136] The Minnesota Supreme Court looked to Section 652D of the Restatement (Second) of Torts to find that an invasion of privacy cause of action requires that the dissemination result in "publicity" of privacy facts.[137] Because the disclosure was internal to other employees, and not to the public at large, the Court held

127. CAL. CIV. CODE § 1798.84(b) (West Supp. 2008); WASH. REV. CODE ANN. § 19.255.010(10)(a) (West 2007).

128. N.H. REV. STAT. ANN. § 359-C:21(I) (Supp. 2007).

129. FLA. STAT. ANN. § 817.5681(10)(b) (West 2005).

130. LA. REV. STAT. ANN. § 51:3075 (2003).

131. NEV. REV. STAT. ANN. § 603A.920 (West Supp. 2007).

132. N.Y. GEN. BUS. LAW § 899-aa(6) (McKinney Supp. 2008).

133. TEX. BUS. & COM. CODE ANN. § 48.201(a) (Vernon Supp. 2007).

134. *See, e.g.*, Bodah v. Lakeville Motor Express Inc., 663 N.W.2d 550 (Minn. 2003); Guin v. Brazos Higher Educ. Serv. Corp. Inc., 2006 WL 288483 (D. Minn. Feb. 7, 2006).

135. 663 N.W.2d 550 (Minn. 2003).

136. *Id.* at 553.

137. *Id.* at 557.

the dissemination was insufficient publicity to support an invasion of privacy claim.[138]

In *Guin v. Brazos Higher Education Services Corp. Inc.*,[139] Guin alleged on behalf of herself, and others similarly situated, that Brazos—Guin's student loan provider—negligently allowed an employee to take unencrypted nonpublic customer data off the company premises on a company issued laptop, which was subsequently stolen from that employee's home during a burglary.[140] In addition to finding that Guin presented no evidence that Brazos breached the duty owed under the Gramm-Leach-Bliley Act it held that the threat of future harm—harm not yet realized—will not support a claim for negligence, which requires a showing of an injury.[141] The court reasoned that Guin presented no evidence that her data was targeted or accessed by the individual(s) who stole the laptop, and as of the date of the court's order, Guin had experienced no instance of identity theft or any other fraud involving her personal information.[142] Thus, the court dismissed his negligence claim.[143]

The element of damages has been a particular problem for plaintiffs in this area.[144] However, depending on the circumstances, where a plaintiff can show a causal connection between the data breach and evidence of identity fraud, he or she may be able to survive summary judgment.[145]

---

138. *Id.* at 557-58.

139. 2006 WL 288483 (D. Minn. Feb. 7, 2006).

140. *Id.* at *1-2.

141. *Id.* at *3-5 (citing Reliance Ins. Co. v. Anderson, 322 N.W. 2d 604, 607 (Minn. 1982) ("the threat of future harm, not yet realized, will not satisfy the damage requirement.")).

142. *Id.* at *6.

143. *Id.* at *7.

144. *See, e.g.*, Pisciotta v. Old Nat'l Bancorp, 499 F.3d 629, 636-637 (7th Cir. 2007) (refusing to award damages for the cost of past and future credit monitoring services that plaintiff obtained as a result of a breach); Bell v. Acxiom Corp., 2006 U.S. Dist. LEXIS 72477, at *6, *8, *10 (E.D. Ark. 2006) (refusing to award damages where plaintiff was unable to show any concrete injuries that resulted form breach); Key v. DSW, Inc., 454 F. Supp. 2d 684, 687-90 (S.D. Ohio 2006) (holding plaintiff, whose injuries were speculative, lacked standing); Stollenwerk v. Tri-West Healthcare Alliance, 2005 U.S. Dist. LEXIS 41054, at *8-9 (D. Ariz. 2005) (refusing to award damages where there is mere exposure of sensitive personal information without evidence of actual injury); Forbes v. Wells Fargo Bank, 420 F. Supp. 2d 1018, 1020-21 (D. Minn. 2006) (granting defendant's summary judgment where the actual injuries alleged—time and money spent to monitor credit accounts for identity theft—"was not the result of any present injury, but rather the anticipation of future injury that has not materialized"). *But see*, Bell v. Mich. Council 25, 2005 Mich. App. LEXIS 353, at 16 (Mich. Ct. App. 2005) (awarding plaintiff damages for injury incurred as a result of breach due to existence of a special relationship between the parties).

145. Stollenwerk v. Tri-West Healthcare Alliance, 254 F. App'x 664, 667 (9th Cir. 2007) (permitting plaintiff to survive summary judgment where plaintiff introduced evidence from which

3. Record Destruction Requirements

Many companies struggle to determine how long to retain certain records. Retaining the information for too short a period may result in a violation of a particular record retention requirement or hamper a company's ability to resolve a particular dispute or defend itself in litigation. However, retaining records for too long a period may unnecessarily expose the records to unauthorized access. Indeed, good record management practices include a comprehensive record retention and destruction policy. In this regard, when companies finally do destroy records, state law requirements prescribe the methods for doing so in order to ensure the personal information in the records can no longer be accessed.[146]

In a number of states, when businesses destroy records containing personal information, they must ensure that the personal information is unreadable.[147] For example, businesses in Texas that dispose of such records must modify the records by shredding, erasing, or any other means so that the personal information is unreadable or undecipherable.[148] Similar laws apply in other states such as New York and California.[149]

Texas Attorney General Greg Abbott recently filed lawsuits against a number of companies alleging that they failed to comply with the state's data privacy and security laws; in particular, for failing to properly dispose of records.[150] On January 10, 2008, Attorney General Abbott filed suit against a company alleging that by disposing sensitive information into trash dumpsters, the company failed to (i) adopt reasonable procedures to protect and safeguard the information, and (ii) properly dispose of the information in violation of Texas law.[151] Attorney General Abbot filed similar suits against two other companies

a jury could infer a causal relationship between theft of hard drives containing personal information and the incidents of identity fraud suffered).

146. *See infra* notes 147-49 and accompanying text.

147. *See, e.g.*, CAL. CIV. CODE § 1798.81 (West Supp. 2008); N.Y. GEN. BUS. LAW § 399-h(2) (McKinney Supp. 2008); TEX. BUS. & COM. CODE ANN. § 35.48(d) (Vernon Supp. 2007).

148. TEX. BUS. & COM. CODE ANN. § 35.48(d) (Vernon Supp. 2007).

149. CAL. CIV. CODE § 1798.81 (West Supp. 2008); N.Y. GEN. BUS. LAW § 399-h(2) (McKinney Supp. 2008).

150. *See infra* notes 151-52.

151. Press Release, Office of the Texas Att'y Gen. Greg Abbott, Texas Att'y Gen. Takes Action Against National Health Servs. Provider to Protect Consumers from Identity Theft (Jan. 10, 2008), *available at* http://www.oag.state.tx.us/oagnews/release.php?id=2345.

in 2007.[152] In July 2008, Attorney General Abbot reached settlement agreements in two of these suits—one settlement required the company to pay $990,000 to the state, and in the other suit, $630,000.[153] In both cases, the companies also agreed to strengthen their existing information security policies by implementing new employee training programs and educating staff about proper document destruction protocols.[154] This kind of enforcement action illustrates that businesses need to be mindful, not only of private lawsuits by affected individuals, but also action taken by State Attorneys General.

III. NEXT STEPS

As businesses and practitioners begin to grapple with these issues, there are some important questions they should be asking themselves in order to assess the risks and the need for further action with regard to safeguarding personal information. That is, in addition to understanding the scope of legal exposure in terms of the availability and amount of penalties and damages under particular laws, by asking some of the questions below and examining the responses, businesses and practitioners likely will be better able to determine appropriate next steps:

> Does the business have a designated officer/committee dedicated to data privacy and security?
>
> What is the volume and nature of personal information accessed, used, maintained and disclosed by the business?
>
> To what extent does the business maintain personal information electronically?

152. *See, e.g.*, Press Release, Office of the Texas Att'y Gen. Greg Abbott, Att'y Gen. Abbott Protects Texas Consumers from Identity Theft (Apr. 2, 2007), *available at* http://www.oag.state.tx.us/oagnews/release.php?id=1961; Press Release, Office of the Texas Att'y Gen. Greg Abbott, Att'y Gen. Abbot Continues Aggressively Enforcing Identity Theft Prevention Law (Apr. 17, 2007), *available at* http://www.oag.state.tx.us/oagnews/release.php?id=1976.

153. Press Release, Office of the Texas Att'y Gen. Greg Abbott, Att'y Gen. Abbot Reaches Agreements That Will Help Protect Texans From Identity Theft (Jul. 16, 2008), *available at* http://www.oag.state.tx.us/oagNews/release.php?id=2554.

154. *Id.*

Has the business conducted an internal audit/risk assessment designed to (i) identify information maintained in the organization that is subject to data privacy and security laws; (ii) map the flow of that information throughout the organization; and (iii) assess the risks of unauthorized access and disclosure? When was that assessment conducted? How frequently are assessments conducted?

Is the company more or less likely to use devices and technology that facilitate remote/wireless access to personal information?

Are members of the business's workforce more likely to access personal information while traveling, working from home, making sales calls, etc.?

In what states does the entity do business?

Has the company had prior breaches of its electronic systems? How were those instances handled?

Does the business have a written plan to address privacy and data security—including policies and procedures regarding when personal information may be received, created, accessed, used, modified, disclosed, discarded? When was it created, updated?

What steps has the business taken to create awareness in the organization regarding the importance of privacy and data security? How often are workforce members trained? Is training documented? Does the business have confidentiality agreements with workforce members?

How prepared is the business to deal with a breach of personal information, including steps to mitigate harm caused by the breach?

Does the business' current insurance cover these risks, including notification and defense costs? Does the business offer data protection services to workforce members, such as credit monitoring, identity theft insurance, identity theft repair services?

How often does the business re-evaluate its privacy and data security policies and procedures?

Does the business have a comprehensive record retention/destruction policy?

This list is by no means exhaustive, but it raises some of the key issues related to the data privacy and security environment in an organization.

IV. CONCLUSION

With instances of identity theft on the rise and personal information increasingly available through various sources, businesses and practitioners need to be aware of their obligations and exposures. In short, businesses must proactively develop an overall strategy for protecting information from unauthorized access and for responding to a breach when it occurs.