BNA

Privacy & Security Law Report®



# Personal Data Breach Notification Laws: How Hard Do You Have to Look?

By Robert L. Rothman and Keith A. Cheresko

*Robert L. Rothman is a Principal of Privacy Associates International LLC and an adjunct professor of law at Thomas M. Cooley Law School. He has taught Privacy Law as an adjunct at Wayne State University and is a former Chief Privacy Officer at General Motors Corporation. Keith A. Cheresko, C.I.P.P., is a Principal of Privacy Associates International LLC. He is the former General Counsel of the Ponemon Institute and the former head privacy lawyer at Ford Motor Company.*

## Executive Overview

A growing body of law around the world requires organizations to put into place physical, technical, and administrative security measures to protect various kinds of personal information. In general, the security measures an organization must adopt are not absolute, but vary depending on the organization's size and complexity, the nature and scope of its activities, and the volume and sensitivity of the personal information involved. Breach notification laws requiring organizations to notify individuals, and often government officials, in the event of an unauthorized accessing or acquisition of specified types of personal information, are also spreading around the world. These laws typically cover situations such as the loss of physical devices on which personal information was stored, unauthorized access to personal information by third parties such as hackers, and unauthorized access to personal information by trusted insiders. Most of these laws require notification within a specified period following the discovery of a breach, yet fail to specify standards on how much time and money must actually go into discovering that a breach has occurred. Under these circumstances, it is appropriate to analogize to the general data security laws and base the level of required breach detection effort on the organization's size and complexity, the nature and scope of its activities, and the volume and sensitivity of the personal information involved. This leads to the logical conclusion that the greater the size of an organization and the greater the sensitivity and volume of personal data it holds, the more extensive and sophisticated the breach detection methods it must use. At

 ISSN 1538-3423

the same time, the more granular the technical breach detection methods employed, the greater the likelihood that only the specific data that was subject to the unauthorized access can be identified, potentially limiting the scope of any breach response action and avoiding cost.

Organizations may be generally aware of their obligation to provide security for personal information that comes into their possession from employees, customers, vendors or other sources. Many may also be aware that they have obligations to notify impacted individuals, and often government officials, in the event of a security breach involving certain types of personal information. However, what may be less clear to organizations is the extent to which they have to put in place processes and systems that allow them to detect when a breach has actually occurred. In other words, how hard does the law require an organization to look for a breach?

This article discusses the standards applicable to general personal information security obligations, breach notification obligations, some of the practical difficulties faced in determining when a breach has occurred, and finally suggests an approach for ascertaining and implementing an organization's breach detection obligations.

## I. Data Security Obligations Under Existing Laws

To a large extent, security obligations in the U.S. have developed primarily along industry lines. In most contexts, protection of consumer information is subject to rules developed by the Federal Trade Commission (FTC).[1] Financial services companies are subject to the Gramm-Leach-Bliley Act (GLBA),[2] the Fair Credit Reporting Act[3] and similar laws and implementing regulations administered by a variety of government agencies, including the FTC. Health care organizations are normally subject to the Health Insurance Portability and Accountability Act (HIPAA),[4] the HIPAA Security Rule[5] and the Health Information Technology for Economic and Clinical Health Act (HITECH)[6] administered primarily by the Department of Health and Human Services. State laws also cover various data security requirements.[7] Despite the existence of all these laws administered by various authorities, the rules have created very similar obligations.

The FTC uses its broad power to prevent ''*unfair or deceptive acts or practices in commerce*''[8] to protect consumer personal information. By bringing actions against companies and either litigating or negotiating settlements, the FTC has been very effective in promoting consumer information security. In early cases the FTC compared the security promises made in the privacy statement of an organization that experienced a security breach to the organization's actual practices. If the actions did not did not conform to the words (i.e. were untrue), the FTC initiated an action based on its power to prevent *deceptive* acts.[9] In more recent situations, in addition to a continued focused on privacy statements, the FTC has maintained that the failure to protect consumer personal information, regardless of what is said, is an *unfair* practice. It now brings legal actions against companies that do not provide adequate security for consumer personal information based on its authority to prevent unfair actions.[10]

The FTC expects an organization to provide physical, technical, and administrative security for consumer personal information.[11] Physical security includes for example facility access controls, safeguarding hard copy documents containing personal information, and securing hardware on which personal information is stored. Technical security relates to protection of electronic personal information through the use of technology. It includes devices such as firewalls, anti-spyware programs, encryption, applications that de-identify personal information, system scanning and similar actions. Finally, administrative security includes the rules and

[1] Federal Trade Commission Act, 15 U.S.C. §§ 45(a)(2), 57a.

[2] Gramm-Leach-Bliley Act, 15 U.S.C. §§ 6801–6810 (hereinafter GLBA).

[3] Fair Credit Reporting Act, 15 U.S.C. §§ 1681 *et seq*.

[4] Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936 [hereinafter HIPAA].

[5] Health and Human Services Security Standards: Final Rule, 45 C.F.R. pts. 160, 162, 164 (2003) [hereinafter HIPAA Security Rule].

[6] Health Information Technology for Economic and Clinical Health (HITECH) Act, Title XIII of Division A and Title IV of Division B of the American Recovery and Reinvestment Act of 2009 (ARRA), Pub. L. 111–5 [hereinafter HITECH Act].

[7] *See, e.g.*, Nevada encryption requirements, Nev. Rev. Stat. § 603A.010 *et seq.* (2009); Rhode Island data destruction statute, R.I. H. 5902 (2009); Massachusetts data protection requirements, Mass. Gen. Laws ch. 93H 201 § 2(a) (2009) and California general information security law, Cal. Civil Code § 1798.81.5(b).

[8] Federal Trade Commission Act, 15 U.S.C. § 45.

[9] *See, e.g.*, *In re Eli Lilly and Co.*, File No. 012 3214 (2002) *available at* http://www.ftc.gov/os/caselist/0123214/0123214.shtm; *In re Microsoft Corp.*, File No. 012 3240, (2002) *available at* http://www.ftc.gov/os/caselist/0123240/0123240.shtm; *In re Guess?, Inc.*, File No. 022 3260 (2003) *available at* http://www.ftc.gov/os/caselist/0223260/index.shtm; *In re MTS, Inc.*, File No. 032-3209 (2004) *available at* http://www.ftc.gov/os/caselist/0323209/0323209.shtm; *In re Petco Animal Supplies, Inc.*, File No. 032 3221 (2005) *available at* http://www.ftc.gov/os/caselist/0323221/0323221.shtm; *In re Guidance Software, Inc.*, File No. 062 3057 (2007) *available at* http://www.ftc.gov/os/caselist/0623057/index.shtm.

[10] *See, e.g.*, *In re BJ's Wholesale Club, Inc.*, File No. 042 3160 (2005), *available at* http://www.ftc.gov/os/caselist/0423160/0423160.shtm; *In re CardSystems Solutions, Inc.*, File No. 052 3148 (2006), *available at* http://www.ftc.gov/os/caselist/0523148/0523148.shtm; *In re Dave & Buster's, Inc.*, File No. 082 3153 (2010), *available at* http://www.ftc.gov/os/caselist/0823153/index.shtm; *In re DSW Inc.*, File No. 052 3096 (2006), *available at* http://www.ftc.gov/os/caselist/0523096/0523096.shtm.

[11] To help communicate these expectations the FTC has created educational materials for businesses. These materials are available through an FTC micro-site, ''Protecting Personal Information: A Guide for Business,'' available at http://www.ftc.gov/bcp/edu/microsites/infosecurity/buttons.html. Among other things the site offers is a downloadable pamphlet, available at http://business.ftc.gov/documents/bus69-protecting-personal-information-guide-business.pdf, and an interactive video tutorial presentation to provide businesses with information about their security obligations. The interactive video is available at http://www.ftc.gov/bcp/edu/multimedia/interactive/infosecurity/index.html. This requirement has also been manifested in FTC settlement orders. *See, e.g.*, Decision and Order at 3, *In re Twitter, Inc.*, File No. 0923093 (2011), *available at* http://www.ftc.gov/os/caselist/0923093/110311twitterdo.pdf. *See also infra* note 12.

  PVLR ISSN 1538-3423

training applicable to personal information handling, including processes to ensure access authorization is only given to individuals with legitimate purposes, authentication rules, rules limiting what data can be stored on portable devices such as laptops and thumb drives, security provisions in supplier contracts, and security training for those with access to personal data.

It is important to note the FTC does not expect every organization to provide the maximum available security in every possible area regardless of cost. Rather, it expects organizations to put in place reasonable safeguards appropriate to the organization's size and complexity, the nature and scope of its activities, and the sensitivity of the personal information involved.[12] The FTC expects risk assessments to be conducted to determine the areas of greatest risk and the areas which would have the most serious consequences in the event a breach were to occur.[13] Reasonable safeguards are then to be put in place in light of those findings. It follows that a large company with a great deal of very sensitive consumer personal information has a different obligation to install physical, technical, and administrative safeguards than a small ''mom and pop'' store with a limited amount of personal information.

Personal information in the hands of financial services companies is regulated in the U.S. on a national level.[14] GLBA required designated financial institution oversight agencies and the FTC to adopt regulations establishing standards relating to physical, technical, and administrative safeguards to address security issues such as the unauthorized access to, or use of, customer information.[15] As a result, several of these federal agencies adopted the Interagency Guidelines Establishing Standards for Safeguarding Customer Information. The guidelines require financial institutions such as national banks to adopt written information security plans.[16] The plans must assess, manage, and control threats that could result in unauthorized disclosure of information.[17] Much like the FTC enforcement-developed consumer personal information rules, the Guidelines encourage financial institutions to adopt measures appropriate to their circumstances.

The FTC also issued standards under GLBA, generally referred to as the Safeguards Rule, applicable to financial institutions for which the FTC has oversight responsibility.[18] These include businesses meeting the broad GLBA definition of financial institution which are not subject to another regulator's oversight such as check-cashing companies, motor vehicle retailers, payday lenders, finance companies, and mortgage brokers. The Safeguards Rule also gives institutions considerable flexibility in implementing safeguards.

On the U.S. state level financial institutions may be regulated by numerous agencies that impose security obligations for the protection of various types of personal information. State regulated banks and insurance companies are examples of the kind of entities that are subject to state regulation.[19]

Security is also an important consideration in the regulation of health care providers. HIPAA, the HIPAA Security Rule and HITECH establish national standards to protect individuals' electronic personal health information in the hands of certain kinds of entities.[20] These standards also require appropriate administrative, physical, and technical safeguards to ensure security of electronic protected health information. In addition to the HIPAA requirements, some states have also enacted legislation for the protection of health information.[21]

Security requirements outside the U.S. did not develop on an industry sector basis, and yet are generally consistent with the American rules. Most countries follow the European Union model of imposing security obligations on those who process personal information in whatever context it arises with few distinctions among general consumer personal data, financial personal data, health care and other similar personal data.[22] This approach has the advantage of avoiding the multitude of different laws, rules, and regulations, as well as the myriad of regulatory authorities, present in the U.S. However, the one size fits all approach results in the disadvantage of a very broad definition of personal information, normally: ''any information related to an identified or identifiable natural person.''[23] The EU Data Protection Directive requires all twenty-seven member states to adopt laws that meet certain stan-

---

[12] FTC enforcement actions impose this requirement. *See, e.g.*, Decision and Order at 2, *In re The TJX Cos., Inc.*, File No. 072-3055 (2008), *available at* http://www.ftc.gov/os/caselist/0723055/080801tjxdo.pdf; Decision and Order at 2, *In re DSW, Inc.*, File No. 052 3096 (2006), *available at* http://www.ftc.gov/os/caselist/0523096/0523096c4157DSWDecisionandOrder.pdf. *See also* FTC Safeguards Rule 16 C.F.R. pt. 314.3(a) (2011).

[13] *See supra* note 11.

[14] *See* GLBA, *supra* note 2 at § 6801(b).

[15] *See* GLBA, *supra* note 2 at §§ 6801(b), 6804(a).

[16] Interagency Guidelines Establishing Standards for Safeguarding Customer Information, 12 C.F.R. ch.1 app. B to pt. 30 (1-1-11), *available at* http://edocket.access.gpo.gov/cfr_2011/janqtr/pdf/12cfr30AppB.pdf

[17] *Id.* at §§ II(A)–(B), III(C).

[18] FTC Safeguards Rule, 16 C.F.R. pt. 314, *available at* http://ecfr.gpoaccess.gov/cgi/t/text/text-idx?c=ecfr&tpl=/ecfrbrowse/Title16/16cfr314_main_02.tpl.

[19] State authorities legislate in this area for state chartered banks, payday lenders, pawn brokers and others. Some states have also imposed general data protection requirements for all businesses that process personal information. *See supra* note 7. In addition, GLBA designated state insurance authorities as the enforcers for compliance with GLBA. *See* GLBA, *supra* note 2 at § 6805.

[20] *See generally*, *supra* notes 4, 5, 6. In addition, the HIPAA Privacy Rule protects all individually identifiable health information held or transmitted by a covered entity or its business associate, in any form or media, whether electronic, paper, or oral. *See* 45 C.F.R. § 160.103, *available at* http://edocket.access.gpo.gov/cfr_2007/octqtr/45cfr160.103.htm.

[21] *See, e.g.*, California - ''Every provider of health care shall establish and implement appropriate administrative, technical, and physical safeguards to protect the privacy of patient's medical information'' (Cal. Health & Safety Code § 130203); Michigan - ''records must be maintained in such a manner as to protect their integrity, to ensure their confidentiality and proper use . . .'' (Mich. Comp. Laws Ann. § 333.16213(1)); and Florida - ''All records owners shall develop and implement policies, standards, and procedures to protect the confidentiality and security of the medical record.'' (Fla. Stat. § 456.057(11) (2009)).

[22] The laws of many countries do distinguish between ''personal data'' and ''sensitive personal data,'' a category of personal data that enjoys special protections.

[23] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals With Regard to the Processing of Personal Data and on the Free Movement of Such Data, Art. 2(a), O.J. (L 281), 23/11/1995 P. 0031 – 0050 [hereinafter ''EU Data Protection Directive''].

dards for data security.[24] The laws must require technical and organizational measures to prevent unauthorized disclosure and access. Further, the measures taken must ensure a level of security appropriate to the risks represented and the nature of the data, taking into consideration the state of the art and the costs of implementation.[25]

## II. Breach Notification Obligations

Laws establishing data security obligations are being supplemented throughout the world with data breach notification laws. These laws are primarily intended to ensure that those whose personal information was subject to a security breach are made aware of the breach so they may take appropriate steps to help protect themselves from identity theft or other adverse consequences. Another purpose of some laws is to make certain specifically designated government officials are notified so they can assist affected individuals and make decisions regarding appropriate enforcement actions. Today, breach notification laws exist in nearly every U.S. state and breach notification requirements are incorporated in certain U.S. federal financial and healthcare information privacy rules.[26] General federal breach notification legislation is also pending in Congress. Outside the U.S., similar laws or regulations exist in Japan, Germany, Austria, Norway, Taiwan, United Arab Emirates, Uruguay and the Canadian province of Alberta.[27] Breach notification legislation is also pending in various other countries. Significantly, the Article 29 Working Party, a body made up of representatives from the data protection authority of each EU Member State, recently issued a Working Paper supporting the inclusion of a breach notification requirement in the anticipated modifications to the EU Data Protection Directive.[28] The EU Justice Commissioner has also announced that she is proposing legislation requiring businesses operating in the EU to inform customers immediately about a serious data breach.[29] Recent amendments to the ePrivacy Directive in the European Union already require all 27 member nations to pass laws requiring breach notification on the part of ''publicly available electronic communication services.''[30] Voluntary codes requiring data breach notification in various forms exist in the UK, Denmark, Ireland, Australia, Hong Kong, New Zealand and Canada (excluding Alberta).[31]

---

[24] *Id.* at Art. 32(1).

[25] *Id.* at Art. 17(1).

[26] All states have enacted breach notification laws except Alabama, Kentucky, New Mexico, and South Dakota. Recently-enacted Texas legislation requires specified entities doing business in Texas that suffer a breach of health-related information to provide breach notification to individuals residing in states without a breach notification law, effectively creating a 50-state breach notification regimen for the protected health information. Texas H.B. 300 § 14(b-1) amending Tex. Bus. & Com. Code § 521.053 (2011). In addition, the District of Columbia, Puerto Rico, and the Virgin Islands have breach notification laws. Regulations adopted pursuant to GLBA and the HITECH Act have established breach notification requirements.

[27] Guidelines for Personal information Protection in the Financial Field Art. 22 (Japan), *available at* http://www.fsa.go.jp/frtc/kenkyu/event/20070424_02.pdf (Unofficial English translation) (last visited Aug. 31, 2011). Under Japan's Financial Services Agency's guidelines breach notification is mandatory. Government authorities must be immediately notified about all data breaches, regardless of their size or severity. Individuals must be notified promptly, and a public announcement must follow. Bundesdatenschutzgesetz [Federal Data Protection Act], Dec. 20, 1990, BDBl I at 2945, as amended in the version promulgated Jan. 14, 2003 (Federal Law Gazette I, p. 66), last amended by Article 1 of the Act of Aug. 14, 2009 (Federal Law Gazette I, p. 2814), in force from Sept. 1, 2009, pt. IV § 42a (Ger.), *available at* http://www.bfdi.bund.de/EN/DataProtectionActs/Artikel/BDSG_idFv01092009.pdf?__blob=publicationFile; Federal Act concerning the Protection of Personal Data (Datenschutzgesetz 2000–DSG 2000) BGBl part I No. 165/1999, on 17 Aug. 1999, as amended (Austria); Act of 14 Apr. 2000 No. 31 Relating to the Processing of Personal Data (Personal Data Act) § 27 (Nor.); Personal Data Protection Act, May 26, 2010 (Taiwan), *see discussion available at* http://www.bakermckenzie.com/RRTaiwanPersonalDataProtectionLawOct10/; Data Protection Law of 2007, Dubai International Financial Centre Law No. 1 of 2007 pt.2, para. 16(4) (U.A.E.), *available at* http://op.bna.com/pl.nsf/r?Open=byul-8lylfx; Ley N 18.331 Protección De Datos Personales Y Acción De ''Habeas Data'' [Protection of Personal Data and ''Habeas Data'' Action] Art. 10 (11 Aug. 2008) (Uru.), *available at* http://www.datospersonales.gub.uy/sitio/leyes/Ley-18.331.pdf and regulation Decreto No. 414/009 [Regulating Decree of 31 Aug. 2009] Art. 8, *available at* http://www.datospersonales.gub.uy/sitio/decretos/Decreto-414-009.pdf; Personal Information Protection Act, Statutes of Alberta 2003, Chap. P-6.5 pt. 3, div. 2, para. 34.1 (current as of May 2010) (Can.-Alta.), *available at* http://www.qp.alberta.ca/574.cfm?page=P06P5.cfm&leg_type=Acts&isbncln=9780779748938.

[28] EU Article 29 Data Protection Working Party Opinion 13/2011 on the Current EU Personal Data Breach Framework and Recommendations for Future Policy Developments, 00683/11/EN, WP 184, adopted, Apr. 5, 2011, *available at* http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp184_en.pdf.

[29] Christopher Williams, *Banks to be Forced to Issue Hacking Warnings*, The Telegraph, June 21, 2011, *available at* http://www.telegraph.co.uk/technology/news/8587289/Banks-to-be-forced-to-issue-hacking-warnings.html.

[30] Directive 2009/136/EC of The European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on Universal Service and Users' Rights Relating to Electronic Communications Networks and Services, Directive 2002/58/EC Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector and Regulation (EC) No. 2006/2004 on Cooperation Between National Authorities Responsible for the Enforcement of Consumer Protection Laws, O.J. (L 337), 18.12.2009, p. 11–36, *available at* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:337:0011:0036:En:PDF. *See also* Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector (Directive on privacy and electronic communications) O.J. (L 201), 31.7.2002, p. 37–47, *available at* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2002:201:0037:0047:EN:PDF.

[31] *See, e.g.*, ICO Guidance on Data Security Breach Management (11 July 2011) (U.K.), *available at*: http://www.ico.gov.uk/SearchResultAsHtml.aspx?cid=95rUt2BtRZQJ&page=http://www.ico.gov.uk/for_organisations/data_protection/~/media/documents/library/Data_Protection/Practical_application/GUIDANCE_ON_DATA_SECURITY_BREACH_MANAGEMENT.ashx&keywords=breach notification (last visited Aug. 26, 2011); Office of the Privacy Commissioner: Guide to Handling Personal Information Security Breaches (Aug. 2008). (Austl.), *available at* http://www.healthprivacy.com.au/doc/Guide_to_breach_notification_OPC.pdf; Privacy Commissioner Privacy Breach Guidelines

  PVLR ISSN 1538-3423

While each of these laws around the world is slightly different in scope and other aspects, the trend toward requiring notification of unauthorized access to personal information is clear.

## III. Events Covered by the Breach Notification Laws

Most breach notification laws are triggered by an ***unauthorized access to or acquisition of*** the kind of personal information covered by the law. Beyond that, there are a series of variables that determine whether the unauthorized access actually falls under the law. Among those variables are:

- The data storage medium involved. Some laws are limited to breaches of computerized information while others are applicable to breaches of both computerized and paper documents.[32]
- Whether encryption was used. Many breach laws include an exemption from notification obligations if the unauthorized access was to encrypted personal information, provided the encryption key was not also compromised. These provisions encourage the use of encryption to protect personal data.[33]
- The kind of personal information accessed.[34]

Different breach notification laws are intended to protect different types of personal data. The breach notification statutes in effect in most U.S. states, for instance, generally have a relatively narrow scope. They typically cover unauthorized access to a name in combination with data such as a social security number or driver's license number or a financial account together with a personal identification number that allows access to the account. Other factors such as DNA profiles, mother's maiden name, tax information, passport numbers, and other assorted data elements may also be present in individual state statutes.[35]

Other U.S. breach notification laws cover particular kinds of personal data. The breach notification provisions of the HITECH Act, for instance, cover the unauthorized access to Protected Health Information.[36] The U.S. Federal Trade Commission's Health Breach Notification Rule covers electronic personal health records.[37] Regulations adopted by financial regulators pursuant to GLBA cover unauthorized access to sensitive customer information held by banks and certain other financial institutions.[38]

European laws passed to comply with the European Union's e-Privacy Directive apply to breaches of personal data held in connection with the provision of publicly available electronic communications services. The new German breach notification law covers specific types of financial information and ''sensitive'' personal data, matters such as race, religion, union membership, and sexual orientation.[39] At the other end of the spectrum is Norway, which requires notice to the government in the event of any breach of personal data, broadly defined as any information relating to an ''identified or identifiable natural person.''[40]

---

(Feb. 2008) (N.Z.), *available at* http://privacy.org.nz/privacy-breach-guidelines-2/?highlight=guidance breach notification (each last visited Aug. 2, 2011); Office of the Privacy Commissioner of Canada: Guidelines for Organizations in Responding to Privacy Breaches (August 2007) (Can.), *available at* http://www.priv.gc.ca/information/guide/2007/gl_070801_02_e.cfm (last visited Aug. 26, 2011); Data Protection Commissioner: Personal Data Security Breach Code of Practice (July 2010) (Ir.), *available at* http://www.dataprotection.ie/docs/7/7/10_-Data_Security_Breach_Code_of_Practice/1082.htm, and Breach Notification Guidance, *available at* http://www.dataprotection.ie/docs/Breach_Notification_Guidance/901.htm (each last visited Aug. 26, 2011).

[32] *See, e.g.*, Limited to computerized data: Arizona (Ariz. Rev. Stat. § 44-7501 para. (A)), Arkansas (Ark. Code Ann. § 4-110-103 para. (1)(A) (2011)), California (Cal. Civ. Code § 1798.82), Connecticut (Conn. Gen. Stat. § 36a-701b(a)), Delaware (Del. Code tit. 6, § 12B-101 para. (1)), Florida (Fla. Stat. § 817.5681 para. (1)(a)), South Carolina (S.C. Code § 39-1-90 para. (D)(1)), and Wyoming (Wyo. Stat. § 40-12-501 para. (a)(i)). States with requirements that extend beyond computerized data: Alaska (Ala. Stat. § 45.48.010 (a)), Connecticut (Conn. Ins. Dept. Bull. IC -25 Sept. 7, 2010); Hawaii (Haw. Rev. Stat. § 487N-2(a)); Indiana (Ind. Code §§ 24-4.9-2-2), North Carolina (N.C. Gen. Stat. § 75-65(a)), Wisconsin (Wis. Stat. § 134.98 (2)(a) (2009–10)), and Massachusetts (Mass. Gen. Laws § 93H-1(a)).

[33] *See, e.g.*, Alaska - encrypted data excluded unless key also compromised (Alaska Stat. § 45.48.090(7)); Connecticut (Conn. Gen. Stat. 36a-701b(a)); Indiana - encrypted data excluded unless key also compromised (Ind. Code §§ 24-4.9-3-1 and 4-1-11-5); Michigan (Mich. Comp. Laws § 445.72 (1)(a), (b)); Minnesota (Minn. Stat. § 325E.61 subdiv. 1(a)); Mississippi (Miss. HB no. 583 § 1 para. 2(a) (2010 Regular Session)); New Jersey (N. J. Stat. Ann § 56:8-161); New York - encrypted data excluded unless key also compromised (N.Y. Gen. Bus. Law § 899-aa(b)); North Dakota (N.D. Cent. Code § 51-30-01 (1); Oregon (Or. Rev. Stat. § 646A .602(11)(a)); Pennsylvania - encrypted data generally excluded subject to further conditions (73 Pa. Con. Stats. Ann. Ch. 43 § 2303(a), (b)); South Carolina (S.C. Code §§ 39-1 -90(A), (D)(1)).

[34] Each jurisdiction defines the type and extent of the personal information subject to protection.

[35] For example, California - physical characteristics or description, passport number, insurance policy number, education, employment, medical information, or health insurance information. (Cal. Civil Code § 1798.80 (e)); Iowa - unique biometric data, such as a fingerprint, retina or iris image, or other unique physical representation or digital representation of biometric data (Iowa Code § 715C.1 (11)(e)); Nebraska - unique biometric data, such as a fingerprint, voice print, or retina or iris image, or other unique physical representations (Neb. Rev. Stat. § 87-802(5)(e)); North Dakota - mother's maiden name (N.D. Cent. Code § 51-30-01 (2)(a)(6)); Oregon - passport number or other United States issued identification number (Or. Rev. Stat. § 646A.602(11)(a)(C)); Texas - mother's maiden name, unique biometric data, including the individual's fingerprint, voice print, and retina or iris image (Tex. Bus. & Com. Code Sec. 521.002 (a)(1)); and Wisconsin - individual's deoxyribonucleic acid profile (DNA) (Wis. Stat. § 134.98 (1)(b)(4)).

[36] HITECH Act, *supra* note 6 at Subtitle D of Division A § 13402.

[37] FTC Health Breach Notification Rule, 16 C.F.R. pt. 318 [hereinafter ''FTC Rule''].

[38] *See supra* notes 16 and 17.

[39] Bundesdatenschutzgesetz [Federal Data Protection Act], Dec. 20, 1990, at § 3 para. 9, as amended (Ger.). The EU privacy directive defines specified kinds of personal information as sensitive and affords a higher degree of control and protection to the individuals to whom the information relates.

[40] Act of 14 April 2000 No. 31 Relating to the Processing of Personal Data (Personal Data Act) § 27 (Nor.), *available at* http://www.legislationline.org/download/action/download/id/1102/file/2e3d6bb37cf550acba8549d9759d.pdf.

In Japan, the Guidelines on the Protection of Personal Information in the Financial Sector cover any personal information in the hands of financial institutions and in the event of a breach requires publicity as well as notice to government authorities and the affected individuals.[41]

The various breach notification laws around the world usually do not distinguish among the kinds of unauthorized accesses to, or acquisitions of, personal information covered. However, breaches generally may be characterized as falling within one of three categories: (1) loss of a physical object such as a computer, thumb drive, paper file or other media on which personal information is stored; (2) access by unauthorized third parties through hacking or some similar means; and (3) access by an employee or other trusted person to information beyond the scope of his or her actual authorization.

## III. Breach Detection Challenges

Before an organization is in a position to give a required notice of a personal information security breach, it must become aware an unauthorized access or acquisition occurred. How this happens depends in large part on factors related to the category of security breach.

### *1. Loss of Physical Media*

Discovering a breach based on the loss of physical media on which personal information was stored is in one sense the easiest situation with which to deal and in another sense the most difficult. It is the easiest in that in most cases the loss of the media or device is clear and someone responsible for the physical object will, sooner or later, realize it is gone. For instance, an employee walks into her office on Monday morning and finds her computer has been stolen. An employee starts to do work on an airplane and suddenly realizes he left his smartphone charging in the terminal. The thumb drive someone knew was in his pocket is no longer there. These and thousands of other situations of physical disappearance leave little question of the possibility of unauthorized acquisition of personal information.

At the same time, the loss of physical media is often one of the most difficult situations in which to ascertain whether an actual breach of personal information has occurred. Since the device on which the data resided is gone, the initial inquiry usually relates to the nature and extent of the data it may have contained. If the device had not been recently backed up, there may be no way to determine for certain what data had been compromised. In that situation it may come down to interviewing people to try to ascertain what, if any, personal information may have been on the device. In some cases the individual will not remember or will not be aware that automatic processes had saved information to the device that he assumed he had completely deleted. This often makes it impossible to know with any certainty whether the type of information that triggers a notification obligation was present. Further, even if the organization determines it is best to assume the missing device held notifiable data, it may well be impossible to determine the specific individuals affected and to whom notices should be sent. This leaves the organization vulnerable to enforcement actions and eventual complaints from those whose information was actually compromised.

Another frequent problem in large organizations is the lack of effective processes and administrative security measures to connect an individual who has lost a physical device containing personal information with those internal personnel who are aware of and understand the organization's legal responsibilities. For instance, an employee unfamiliar with or untrained in his breach notification responsibilities may lose a thumb drive on which personal information is stored, but because the object itself is so inexpensive he will not bother to report the loss, thus exposing affected individuals to possible identity theft. In addition, the failure to report may ultimately place the organization in a non-compliant situation and expose it to fines, penalties, and complaints.

### *2. Access by Unauthorized Third Parties*

Discovering a breach caused by an unauthorized third party, such as a hacker, is more or less likely based on numerous technical factors. At the highest level these include the nature of the system being attacked: is it composed of a single computer, a distributed network, or a mainframe? It may be somewhat more likely that a breach will be detected on a mainframe system simply because the costly device is more likely to be watched over by trained system security administrators, employ sophisticated security devices, apply ''patches'' and use software to detect or prevent intrusions. Even then it certainly is not invulnerable to attack. Detecting a breach on a single computer or small network employed by organizations whose core business is outside the technical IT area may be somewhat less likely simply because not as much attention and investment is normally devoted to the problem. Of course, there are certainly exceptions.

Regardless of the type of system, the standard method for determining whether a third party breach has occurred is through utilization of intrusion detection and prevention software and logging. Intrusion detection and prevention systems attempt to identify possible incidents, log information about the incident, try to stop the intrusion, and report the event to security administrators. Logging events through a computer operating system or other program provides an audit trail that can be used to understand system activity at some level. Of course, for logging to work it has to be turned on and monitored. Yet because logging can deteriorate system performance that does not always occur. Additionally, most logging is not performed at a sufficiently granular level to determine exactly what occurred beyond the fact a specific file was accessed by a specific user at a specific time. For instance, if all the log reveals is that a specific identification number accessed a certain database containing personal information of one thousand individuals at a specific time, the information of all thousand people must be considered as breached. On the other hand, if the system can determine not only that the database was accessed, but also that only the information on five individuals was reviewed or acquired, only the information on those five individuals would have to be considered to have been breached. This can make a significant difference both in terms of

[41] Guidelines for Personal information Protection in the Financial Field (Japan), *available at* http://www.fsa.go.jp/frtc/kenkyu/event/20070424_02.pdf (Unofficial English translation).

  PVLR ISSN 1538-3423

direct breach notification costs and indirect costs such as adverse publicity and loss of goodwill.[42].

There are many issues and complexities surrounding logging but one of the primary difficulties stems from the sheer volume of information created and the problems associated with interpreting the entries, particularly when the reviewer is not looking for some particular event.[43] Intrusion detection and prevention systems can narrow the focus of logs that must be reviewed, but may not provide sufficient detail to know with certainty the scope of the intrusion. Log reviews can be costly manual operations where individual technicians look through very large volumes of information for patterns and anomalies which can be difficult to detect.

Antivirus software on a single computer or on portions of a distributed system may be able to detect that malware capable of allowing third party access to personal information was installed, but it generally cannot determine whether access to specific data actually occurred. Thus, these systems are normally good protection devices, but of very limited usefulness in determining whether a breach actually occurred.

### *3. Access by Insiders*

Discovering a data breach by employees or other trusted insiders who have authorized access to a system can be more difficult than discovering a breach by an outside third party. Large, technically sophisticated companies are likely to have role-based controls to limit an individual's access to areas of a system he is not authorized to enter. However, that is not always the case with respect to smaller companies. Also, as in the case of intrusion by outside third parties, log reviews may be able to reveal what files or databases were accessed after an authorized logon, but normally do not reveal what actually occurred when the user was in the database. This lack of detailed information may make it difficult or impossible to limit the scope of a breach event to information that was *in fact* accessed and instead require notification to everyone whose data *may have been* accessed. As noted above, this distinction can be financially quite significant to an organization.

Breach detection in large companies presents other challenges as well. Depending on the structure of the systems involved, users such as system and security administrators, programmers, application developers and even helpdesk personnel often must have authorized access to large portions or even the entire network to do their work. Determining whether these kinds of individuals have accessed personal data for improper purposes can be extremely difficult without tools that go beyond simple logging. Programs such as keystroke loggers that record employee's every action are certainly available, however at some point the protection of the personal information in the system will start to infringe the privacy of the employee. The answer to this dilemma may well be to utilize systems and processes that are narrowly tailored to address the data protection issue while at the same time limiting any unnecessary effect on employees. For instance, for processing personal information:

- Any system utilized should be able to record exactly what the user has done after accessing a database or file containing personal information. In the event of the use of the personal information by an authorized user for improper purposes, notices could then be sent only to those individuals actually affected, not to everyone in the database. From the organization's standpoint this will serve to limit the adverse financial and publicity impacts of the breach. From a societal standpoint it will help limit the ''breach notice fatigue'' that comes from receiving many unnecessary notices, leading to a reduction in their overall effectiveness.

- The system should be application-based and not employee-based. That is, the system may record the activity of every employee while he is accessing the file or database containing personal information, but should not routinely record all actions of any particular employee without some other cause. This will help demonstrate that the purpose of the recording is to protect the personal information in the database, not impinge on the employee's privacy.

- Clear notice should be given to employees disclosing a recording system is in operation and explaining what it does and why it is necessary. In the U.S. this will serve to eliminate any employee ''expectation of privacy.'' In Europe and other countries with European-style legislation notice will help demonstrate the ''fairness'' of the processing to data protection authorities and works councils. This is particularly important in light of the fact that the European breach notification laws that do now exist are new and there has not yet been much focus on balancing the obligations of organizations to give breach notices and the methods of obtaining the necessary information to do so.[44] Accurate notices to employees of the existence and use of the recording systems will also have the advantage of deterring improper utilization of personal information to which they have authorized access.

## IV. Determining the Breach Detection Obligation

In general breach notification laws stipulate that the required notice must be given within some specified period *after the breach has been discovered*. That period may be described as a ''reasonable'' period or as a

[42] Having more precise information obtained through logging can have a major impact on the cost and reputation to an organization experiencing a breach. According to the Ponemon Institute's 2010 Annual U.S. Cost of a Data Breach Study, March 2011, the average cost per compromised record for 2010 was $214. So the difference between the compromise of 10 records ($2,140) and 1000 records ($214,000) can be significant. Ponemon Institute, LLC, *2010 Annual Study: U.S. Cost of a Data Breach* (March 2011), *available at* http://www.symantec.com/content/en/us/about/media/pdfs/symantec_ponemon_data_breach_costs_report.pdf

[43] According to the 2010 Data Breach Investigations Report by the Verizon RISK team in cooperation with the United States Secret Service 87% of organizations had evidence of the breach in their log files, yet missed it. Verizon RISK Team & U.S. Secret Service, *2010 Data Breach Investigations Report*, *available at* http://www.verizonbusiness.com/resources/reports/rp_2010-data-breach-report_en_xg.pdf.

[44] *See supra* note 28.

specified number of days, sometimes as short as five.[45] Some statutes provide for a period of investigation if a breach is suspected and others allow for suspension of notification if the notice will impede law enforcement. In general, however, rules are drafted so the period is measured from the breach discovery.[46]

This raises the question of whether an organization may circumvent the breach notification process in its entirety by adopting an ostrich approach. That is, can an organization simply take no breach detection measures at all and by avoiding knowledge that a breach occurred bypass all the subsequent legal obligations that are triggered from that knowledge? The ostrich approach may initially appear quite attractive in view of the difficulty and expense of actually identifying breaches. However, it is unlikely to work, either legally or practically. A few laws and regulations such as HITECH and the FTC's Health Breach Notification Rule actually define organizations' breach notification responsibilities to commence at the point the breach is known **"or reasonably should have been known."**[47] Surprisingly, the majority of rules and pending legislative measures do not include that kind of imputed knowledge provision. However, even in the absence of a legislative standard, it is unlikely courts in any jurisdiction would allow an organization to use bad faith and ''hide its head in the sand'' with respect to avoiding discovery of unauthorized accesses to personal information. This reluctance would be further accentuated if it could be shown that the norm for similar entities is to provide some level of breach detection. More importantly, an organization that should have known it experienced a breach of personal information and did nothing to help protect the individuals involved may have a high price to pay in terms of image, stakeholder goodwill and regulator relationships.

If organizations holding personal information cannot take actions to actively avoid knowledge that a breach has occurred, should the law impose breach notification obligations only on those unfortunate organizations that happen to stumble on the knowledge of the breach, or should there be some legal obligation to detect breaches? If there is a legal obligation to detect breaches, how much money and other resources should an organization be required to expend to meet the obligation? Should there be a difference in this regard between large companies with significant resources and small companies with limited resources if both are handling the same kind of information? What if they are in direct competition with each other? These are more difficult questions.

Although there do not yet appear to be any reported court decisions on the issue, one logical answer might be found by looking at the approach adopted for protecting personal information in the first place. All organizations must protect personal information. The specific measures the law requires an organization to adopt in this regard are dependent on the organization's size and complexity, the nature and scope of its activities, and the sensitivity of the personal information involved.[48] It follows that the same factors could be used to determine the effort to be put into breach detection. This means large organizations with significant amounts of sensitive personal information, such as financial information or health care information, would have an obligation to put in place sophisticated systems and processes to be able to detect unauthorized accesses or acquisitions to the information. The mom and pop store with small amounts of personal information of limited sensitivity may not need to meet the same high standard, but neither could it ignore the matter of breach detection. Measures should be adopted that allow detection of the most likely and most significant types of breaches.

## V. Implementing a Breach Detection Program

A breach detection program should obviously only be a part of a more general data security program and must be considered in that context. Any organization needs written policies and procedures to let employees know what is expected of them in the event of a breach of personal information, whether it is a physical breach or a technical breach. Contracts with service providers and other third parties having access to personal information must not only include proper provisions to make certain the data is protected, but also to make certain notice is given expeditiously to specifically identified persons if a breach does occur or is suspected. For many organizations, breach detection and application auditing systems should also be utilized.

Each organization, regardless of size, should undergo and document a process to determine exactly what level of breach detection is appropriate for the organization given the considerations discussed above. This process should involve IT professionals, lawyers, privacy and physical security experts, financial representatives and management. Activities might include risk assessments, benchmarking of analogous organizations in the same industry and financial modeling to look at the likelihood and direct and indirect costs of hypothetical breaches and compare those costs with measures and technology that could prevent or mitigate the scope of a breach.

## VI. Conclusion

We are unlikely to see any time soon an abatement of the global trend toward the promulgation of laws requiring the protection of personal information. Further, since information security can never be perfect regardless of what legislation is in place, breach notification laws that attempt to assist with lapses in security are also likely here to stay. Organizations today are forced to deal the problem of how many resources they should, or must, devote to detecting breaches involving per-

[45] California requires certain specified covered health care entities to report any unlawful or unauthorized access to, or use or disclosure of, a patient's medical information to its designated state health authorities and the patient or the patient's representative no later than five business days after detection of the unlawful or unauthorized access, use, or disclosure. Cal. Health & Safety Code § 1280.15(b).

[46] *See, e.g.*, Alaska - after discovering or being notified of the breach (Alaska Stat. § 45.48.010 (a)); California - following discovery or notification of the breach (Cal. Civ. Code § 1798.82 (a)); Indiana - after discovering or being notified of a breach (Ind. Code § 24-4.9-3-1(a)); Texas - after discovering or receiving notification of the breach (Tex. Bus. & Com. Code § 521.053).

[47] *See* HITECH Act, *supra* note 6 at § 13402(c); *see also* FTC Rule, *supra* note 37 at 318.3(c).

[48] *See* discussion *supra* notes 11–13.

  PVLR ISSN 1538-3423

sonal information. For the organization holding personal information this is not a trivial issue. The growing complexity of information technology and sophistication of individuals seeking to obtain unauthorized access to personal information makes actually detecting breaches a complex, and oftentimes expensive process. This places a particularly difficult burden on small organizations not in the information technology arena that deal with sensitive personal information. Furthermore, since the consequences of discovering a breach are so negative in terms of expense and loss of goodwill, organizations have a natural proclivity to minimize efforts to identify breaches. On the other hand, for the individual whose information was the subject of an unauthorized disclosure and is therefore facing the prospect of identity theft and other negative consequences, it is not important whether the breach emanated from a large or small organization. His interest is to be notified of the breach as soon as possible so he can take actions to protect himself.

This article suggests one approach to balancing these various interests. It also suggests some advantages of utilizing technology to help minimize the consequences of certain types of breaches by more specifically identifying the details of a particular breach. But even here there are competing interests between the privacy rights of individuals whose personal information is being retained and the privacy rights of employees who are the stewards of that information.

To date, organizations have had only minimal direction from governments on their breach detection obligations. It is time that the question be more widely debated and conclusions reached by governments, harmonized to the maximum extent, giving firm and equitable direction to holders of personal information.