Washington Journal of Law, Technology & Arts

Volume 3 | Issue 2 Article 3

12-4-2006

To Serve and Protect: Do Businesses Have a Legal Duty to Protect Collections of Personal Information?

Derek A. Bishop

TOPIC
Cite as: Derek A. Bishop, *To Serve and Protect: Do Businesses Have a Legal Duty to Protect Collections of Personal Information?*, 3 Shidler J. L. Com. & Tech. 7 (Dec. 4, 2006), *at* <http://www.lctjournal.washington.edu/Vol3/a007Bishop.html>

TO SERVE AND PROTECT: DO BUSINESSES HAVE A LEGAL DUTY TO PROTECT COLLECTIONS OF PERSONAL INFORMATION?

Derek A. Bishop[1]

Abstract

Commercial, governmental, and nonprofit organizations are more frequently reporting instances of data security breaches. This has, in turn, raised fears of identity theft. In some limited instances, companies that maintain large amounts of personal information — such as credit reporting agencies — have been subject to statutory duties to protect that personal information. In some instances, such legislation has also permitted a private cause of action for breach of these duties. Legislatures have expanded these statutes to encompass, at least to a limited degree, all business entities that collect personal information. Recent precedent indicates that courts may follow this trend by declaring security breaches generally foreseeable, and finding a common law duty on the part of companies to protect their data. The ability of a plaintiff to prove compensable harm from the negligent release of personal information, however, may be more difficult than showing the existence of a duty.

Table of Contents

INTRODUCTION

<1> On February 15, 2005, Choicepoint, a commercial data aggregator,[2] informed 145,000 people that thieves had improperly accessed their personal data.[3] Within the week, a putative class of 145,000 people filed a class action lawsuit against Choicepoint.[4] The plaintiffs alleged, in part, that Choicepoint had negligently released credit reports to unauthorized parties in violation of the Fair Credit Reporting Act ("FCRA"). [5] The FCRA prohibits disclosure of consumer reports from a credit-reporting agency except where requested by the consumer, a law enforcement agency, a court order, or a business for a legitimate business need.[6]

<2> Plaintiffs allege that Choicepoint violated the FCRA by failing to take and maintain reasonable measures in screening the companies that access the plaintiffs' personal data.[7] Then in June, CardSystems, Inc., a credit card processor, acknowledged that thieves had accessed files containing 40 million individuals' credit card information.[8] Soon thereafter, a putative class of 40 million people filed suit against the credit card processor.[9] This lawsuit alleges that CardSystems, Inc. was negligent by failing to adequately secure the personal data.[10] CardSystems has a policy that requires notifying individuals only if thieves misuse the stolen personal information. The plaintiff class alleges that this policy violates California law, because under that state's law, all breaches require notification to affected consumers.[11]

<3> These incidents are part of a broader trend.[12] There were 130 reported security breaches exposing the personal information of 55 million Americans in 2005.[13] Congress, through legislation such as the FCRA, the Health Insurance Portability and Accountability Act ("HIPAA") and the Gramm Leach Bliley Act ("GLBA"), has imposed an affirmative duty on specific industries to protect personal data. State legislatures, by contrast, recently began enacting legislation that impacts most businesses, but imposes a less onerous duty — the duty to notify individuals in the event of a security breach.

<4> Like legislatures, courts are signaling some willingness to impose a common law duty of care to protect personal information. For a court to hold a company liable for negligence under the common law, a plaintiff must prove four elements: the presence of a duty, a breach of that duty, causation, and damages resulting from the breach that are legally compensable.[14] The rise of computer use affects whether companies have a duty to protect personal information, and

whether injuries from the release of personal information are compensable.[15]

<5> The imposition of a duty in tort requires that the risk be foreseeable by the party. Illegal acts, such as data theft, are less foreseeable than simple negligence.[16] Recently, courts have begun to acknowledge the foreseeability of data theft where the company has created a risk of data theft to the individual.[17] Once a court acknowledges the foreseeability of this theft, it will likely impose a duty to protect personal information against the foreseeable risk of theft of such information.

THE EXPANSION OF PERSONAL DATA USE AND MISUSE IN THE INFORMATION AGE

<6> Personal information has gained value in the information age. Companies now collect and sell personal information for a wide range of purposes. These purposes include managing risk, market research, marketing, personalizing online shopping experiences and facilitating income tax withholding. However, this personal information can also be used for illicit purposes. A credit card number can be used illegally to make purchases online, or a social security number may be used to fraudulently open, and borrow on, a line of credit. With the emergence of electronic technologies, the opportunities to steal and illegally use personal information are increasing.[18]

<7> There are significant direct costs associated with the identity theft, and those costs are increasing every year.[19] Direct costs of identity theft include losses stemming from fraudulent transactions, such as goods purchased with a fraudulent credit card. One report, prepared for the Federal Trade Commission, estimated the direct costs to individuals and financial institutions to be $50 billion per year.[20] Actual losses are difficult to calculate because organizations are not required to report economic losses arising from security breaches to customers or other parties.

STATUTORY DUTIES IMPOSED ON COLLECTORS OF PERSONAL DATA

<8> Legislatures play a crucial role in creating duties to protect consumers from data theft. Historically, only companies in fields that acquired and maintained large amounts of personal information as part of their ongoing relationship with consumers were subject to regulations requiring the protection of this data, (e.g., credit agencies,[21] health care institutions,[22] and state

motor vehicles departments).[23] The FCRA,[24] HIPAA,[25] and GLBA[26] are examples of such regulation. These statutes do not generally provide an explicit private cause of action,[27] but the specific duties they place on holders of personal information will likely impact any judicially-imposed duties of care for protecting personal information.[28]

<9> Congress passed the Privacy Act in 1974.[29] It imposes duties only on federal agencies, not on state governments, thus limiting its scope significantly.[30] The Privacy Act requires that federal agencies establish appropriate safeguards to protect personal information held by the agency.[31] Unlike GLBA and HIPAA, it does not create a duty for a company to take specific actions to secure information. Instead it relies on a generic duty to protect.[32] The Privacy Act also provides an explicit private cause of action in contrast to other federal privacy statutes.[33]

<10> More recently, Congress and state legislatures have begun to create affirmative duties for a broader class of organizations that maintain personal data. In most instances this consisted only of a duty to notify individuals whose information was exposed due to a security breach.[34] However, some states, including California, have imposed an affirmative duty on a wide range of businesses to protect personal information.

<11> California is among the first states to enact legislation that imposes security duties on all organizations that maintain personal information.[35] The two houses of its legislature passed two pieces of legislation, Senate Bill ("S.B.") 1386,[36] and Assembly Bill ("A.B.") 1950.[37] These laws create a series of affirmative duties to secure personal data for all companies that maintain the personal information of one or more California residents.[38] These duties include notifying individuals when their information is released, either purposefully or inadvertently.[39] It also requires companies to "provide reasonable security" for personal information, including developing and implementing "reasonable security measures" for protecting the information.[40] It further requires that an organization's subcontractors also implement such measures. [41]

<12> HIPAA creates a duty on healthcare providers and insurers to enact security procedures to protect the personal information of patients.[42] As part of this regulation, HIPAA requires that companies and providers secure protected patient information, and guard against any reasonably anticipated threats or unauthorized uses.[43] HIPAA is unique, however, because

through its "Security Rule," the statute provides 18 different standards that constitute required protection.[44]

<13> GLBA, like HIPAA, is a comprehensive regulatory scheme that imposes a duty on financial institutions to implement reasonable security measures to protect personal information.[45] The Federal Trade Commission has issued regulations, collectively referred to as the "Safeguards Rule," that lists required security measures which must be taken to comply with GLBA.[46] The Safeguards Rule requires each covered organization to develop a written security program that addresses administrative, technical and physical safeguards that the company is taking to secure personal data.[47]

DUTY TO PROTECT PERSONAL DATA UNDER THE COMMON LAW

<14> In tort law, actors generally do not have an affirmative duty to act to protect others.[48] However, an actor can be negligent if his actions create an unreasonable risk of harm to another through the conduct of a third person, even if that conduct is illegal.[49] For example, the theft of "valuable property . . . left unguarded and exposed to the public view" is foreseeable; a duty thus exists to protect that property.[50]

<15> Courts are beginning to consider whether companies have an affirmative duty to protect personal data from release and subsequent illegal use. The New Hampshire Supreme Court considered this question in *Remsberg v. Docusearch*.[51] In that case, a man obtained personal information from Docusearch, an information broker, which he used to stalk and kill a woman.[52] The court considered whether an information broker owed a duty of care to the person whose information they sold when the information was ultimately used for an illegal purpose.[53] The court found that Docusearch had a duty to protect the personal data that it collected from use in an illegal activity.[54] This duty was created in large part due to the foreseeability that the information would be used for illegal purposes.[55] The court specifically addressed the foreseeability of both stalking and identity theft.[56]

<16> At least one appellate court has found that a foreseeable theft of personal information may give rise to a duty of care to protect that information.[57] In an unpublished opinion, *Bell v. Michigan Council 25*, the Michigan Court of Appeals held that a union owed a duty of care to its members to protect their personal information from theft.[58] The union allowed paper files

containing members' personal information to leave the premises, where the daughter of an employee stole the information contained within them.[59] The court found that the theft of the information was foreseeable, and the failure to protect against that theft amounted to a breach of the union's duty of care.[60] As a result of this breach, the court allowed the plaintiffs to collect $275,000.[61]

<17> In both *Bell* and *Remsberg*, the courts recognized that companies generally have no duty to protect against the illegal acts of third parties.[62] In *Remsberg*, the information was used to stalk and kill the individual whose information was released.[63] In Bell, the information was subsequently used to appropriate the plaintiffs' identities.[64] Both the New Hampshire Supreme Court and the Michigan Court of Appeals held that the illegal use of personal information was foreseeable, and subsequently imposed a duty to protect this information from illegal activity.

<18> Recently, in *Poli v. Mountain Valleys Health Centers, Inc*[65]., the U.S. District Court for the Eastern District of California considered the existence of HIPAA and common law causes of action for the release of personal information. Poli's employer, Mountain Valleys Health Centers, was investigating Poli for possession of non-prescribed prescription medication.[66] As part of this investigation, Rite Aid released plaintiff's medical records to Mountain Valleys Health Centers without Poli's permission.[67] The plaintiff asserted causes of action against Rite Aid for violating HIPAA and for common law negligence.[68] The court granted defendant Rite Aid's motion to dismiss the claim for a violation of HIPAA, holding that HIPAA does not create a private cause of action.[69] However, the court refused to dismiss the common law negligence claim.[70] Regarding that claim, the court held that the plaintiff's allegation that a duty existed was sufficient to survive the motion to dismiss.[71]

Foreseeability of Data Collection Resulting in Data Theft

<19> The most significant factor to consider in determining whether a duty to protect personal information exists is the foreseeability of the harm to the plaintiff.[72] In general, actors are not expected to predict the illegal acts of third parties.[73] However, misconduct is foreseeable when a company acts "with the knowledge of peculiar conditions [that] create a high degree of risk of intentional misconduct."[74] In *Remsburg v.*

Docusearch, Inc., the court held that the risk of criminal misconduct is sufficiently foreseeable to impose a duty of care.[75] In coming to this conclusion, it recognized the increasing incidence of both stalking and identity theft, and the public policies that resulted from that increase.[76] Although the opinion addressed a situation where a company intentionally released this information, the court's holding was not limited to those facts but instead hinged on the foreseeability of the illegal actions.[77]

<20> Both the Supreme Court of New Hampshire and the Court of Appeals of Michigan have acknowledged the foreseeability of harm in a negligence context. Tribunals at all levels have begun to acknowledge the foreseeability of harm from security breaches in related contexts.[78] For example, the Maine Public Utilities Commission found that the disruption of computer service due to a computer virus was foreseeable.[79] Because it was foreseeable, Verizon's failure to protect its network did not excuse its inability to meet the promised performance metrics.[80]

<21> Similarly, as part of the ongoing *Cobell v. Norton* litigation, the U.S. Court of Appeals for the District of Columbia Circuit has acknowledged the foreseeability of data theft. [81] This litigation attempts to make the United States government account for billions of dollars held in trust accounts for more than 500,000 Native Americans.[82] To do this, the federal government created a database containing personal information of these citizens. The government was originally enjoined from connecting this database to any network, until they could prove that it was secure. Although the D.C. Circuit lifted the injunction on narrow procedural grounds, it acknowledged that the government had a duty to protect the personal information from outside attack.[83] Although these cases do not directly address questions of negligence, by acknowledging the foreseeability of data theft, the cases may indicate a possible change in the common law that imposes greater duties on companies to protect data stored with them in electronic form.

ESTABLISHING STANDARDS OF CARE FOR DATA SECURITY

<22> The collection of personal data in large databases and the subsequent theft of that information are still relatively new phenomena. As such, there are few fixed standards of care for data security. However, the guidelines of federal agencies tasked with enforcing statutory duties, as well as customer and trade practice, may be indicators of how standards of care for

data protection will be shaped.

<23> A court may review standards of care adopted by Congress and other state legislatures to determine the appropriate standard of care for new common law duties. GLBA and HIPAA have several areas of overlapping requirements that a court may find especially significant in determining the appropriate standard of care. For example, both require that only authorized employees have access to personal data.[84] In addition, each requires that data, including electronic data on workstations, be disposed of properly.[85] Covered entities can also establish an auditing program that is able to detect and repair any unauthorized changes or release of personal information.[86] A review of HIPAA and GLBA may be effective in creating a plan to comply with the emerging duty of care that may be imposed on holders of personal information.

<24> Courts have also provided some guidance as to what precautions are reasonable. For example, in *Bell*, the court found that the union's actions in allowing its member's files to leave the premises helped make the theft of that data foreseeable.[87] If the union had secured the information on the premises, it may have prevented the loss and the ensuing liability. In other cases, courts have found that a provider of personal information, rather than conducting a cursory investigation, should take proactive steps to ensure that the information is going to be used for a legitimate purpose.[88] Another court mandated that a collecting agency create a security plan before having the right to connect to the Internet.[89] These cases instruct that a company would be wise to design a security plan, secure all personal data files, and carefully regulate those who have access to such data.

CONCLUSION

<25> The area of tort liability for security breaches of personal data is still in relative infancy. Legislatures are moving more rapidly than courts in safeguarding personal information by imposing protective duties on several industries that deal with personal data commercially. Other wider-ranging duties have been legislatively proposed. In a recent turn of events, courts have indicated that they may follow suit by finding that companies have a duty to protect private information if the theft of that information is foreseeable.[90] This is largely because data theft and misuse have become increasingly foreseeable,[91] thereby fulfilling a classic prong in tort law. Even if plaintiffs can overcome the duty hurdle, they must prove physical (or other

compensable) damages. This second possible hurdle to a claim notwithstanding, companies should safeguard their customers' private information or risk paying damages for negligence.

PRACTICE POINTERS

- Where possible, encrypt any personal data held by an organization.
- Limit employee travel with laptops that contain personal data, as the loss of a laptop can defeat an organization's security protocols.
- Every organization should conduct a risk assessment that complies with HIPAA and GLBA requirements. This assessment should identify all personal data maintained by the organization and any vulnerability in the organization's systems.
- Limit employee access to personal data. An employee should not access personal data beyond what is necessary for business purposes.
- Dispose of all personal data securely (including shredding paperwork) and destroy any electronic databases.
- Establish an auditing program to track any release or corruption of personal data.

<< Top

Footnotes

1. Derek A. Bishop, University of Washington School of Law, Class of 2007. Thank you to Evgenia Fkarias, Professor Anita Ramasastry, University of Washington School of Law, Mark Melodia, Partner with the law firm of Reed Smith, LLP. and Chris Hoofnagle, Senior Fellow to the Berkeley Center for Law and Technology for their advice and guidance. Thank you to Jennifer Campbell for her constant inspiration.
2. Choicepoint, like other commercial data aggregators, collects an individual's personal information from a wide variety of sources. It then sells this data to third parties, who then use this information to manage various business risks. The classic example is through a credit report, but data aggregators also

process criminal background checks, insurance claims information, and DNA identification. For more information about the breadth of Choicepoint's reach, *see* Choicepoint Inc., Annual Report (Form 10-K), (March 14, 2006).

3. Harry R. Weber, *Choicepoint Review Taps TSA Expert; Media: Data Broker, Reeling from Security Breach Hires Airport Screening Agency Official*, LONG BEACH PRESS TELEGRAM, Mar. 9, 2005, at A19.

4. Tresa Baldas, *Data" Fear Factor": Identity Thefts Lead to Suits; Defining Damages Is at Issue*, NAT'L L. J., May 9, 2005 at 1.

5. First Amended Class Action Complaint at 15, Harrington v. Choicepoint, Inc., No. CV05 1294 SJO JWJx (C.D. Cal. filed Feb. 22, 2005).

6. *See* The Fair Credit Reporting Act, 15 U.S.C. § 1681b (2003).

7. Thieves posing as legitimate business owners accessed the database maintained by Choicepoint and obtained information collected by Choicepoint on 145,000 individuals. The plaintiffs in the class action allege that Choicepoint failed to institute proper safeguards to control access to their data. They further allege that this failure allowed the criminals to access the individuals' data without consent. This access to the individuals' data amounted to a release of a consumer report without a legitimate business need, or the consumer's consent. The plaintiffs allege that this violated the FCRA.

8. Jonathan Krim & Michael Barbaro, *40 Million Credit Card Numbers Hacked: Data Breached at Processing Center*, WASH. POST, June 18, 2005 at A01.

9. First Amended Complaint for Declaratory and Injunctive Relief and Damages at 2, 7 and 12, Parke v. Cardsystems Solutions, Inc., No. CGC-05-442624 (Cal. Super. Ct. July 5, 2005), *available at* http://www.techfirm.com/cardsystems.pdf.

10. *Id*. at 2, 5, 12, 19-20, 23, and 25.

11. *Id* .at 9, 12-13, 26, 27. The court must decide not only when notification must be given, but also by whom notification must be given. The California law is unclear as to what party (i.e. the processor, the banks or other parties) must give notice of the

breach.

12. *See* Beth Givens, *The Information Marketplace: Merging and Exchanging Consumer Data*, Privacy Rts. Clearinghouse, Apr. 30, 2001, http://www.ftc.gov/bcp/workshops/infomktplace/comments/givens.h .

13. Jon Swartz, *2005 Worst Year for Breaches of Computer Security*, USA Today, December 29, 2005 at 1B, *available at* http://www.usatoday.com/tech/news/computersecurity/2005-12-28-computer-security_x.htm?csp=34. For a more in-depth discussion of the types and severity of security breaches *see* Neal G. Walters, *Into the Breach: Security Breaches and Identity Theft*, AARP Public Policy Institute, July 2006, *available at* http://assets.aarp.org/rgcenter/consume/dd142_security_breach.pdf .

14. *See* Restatement (second) of Torts §328A (1965).

15. The "Economic Loss" Rule prevents a plaintiff from collecting damages based on purely economic losses. Courts have begun to consider whether the release of personal information should be an exception to the "Economic Loss" Rule. For further discussion of the "Economic Loss" rule in the release of personal data, see Vincent R. Johnson, *Cybersecurity, Identity Theft, and the Limits of Tort Liability*, 57 S.C. L. Rev. 255 (2005). The negligent release of information that does result in physical harm is compensable in tort. *See* Remsberg v. Docusearch, Inc., 149 N.H. 148, 816 A.2d 1001 (2002).

16. Restatement (second) of Torts §302B cmt. d (1965).

17. *See* Remsburg v. Docusearch, Inc., 149 N.H. 148, 816 A.2d 1001 (2002); Bell v. Mich. Council 25 of the Am. Fed'n of State, County, and Mun. Employees, 2005 WL 356306 (Mich. Ct. of App. 2005) (unpublished); Poli v. Mountain Valleys Health Ctrs, Inc., 2006 WL 83378 (E.D. Cal. 2006) (unpublished); In re Verizon Related Reduction Claim, State of Maine Public Utilities Commission, Docket No. 2000-849 (April 30, 2003); Cobell v. Norton, 391 F.3d 251 (D.C. Cir. 2004).

18. Swartz, *supra* note 13.

19. In addition to direct losses, there are indirect costs caused by the threat of identity theft. Fear of

identity theft prevents some individuals from using online services which significantly lower the cost per transaction. An online banking transaction costs a bank an average of $0.015, where an average traditional transaction costs $1.07. *See* Luxman Nathan, *www.your-community-bank.com:Community Banks Are Going Online*, Communities and Banking, Nat'l Reserve Bank of Boston, Boston, MA, Fall 1999, at 3, *available at* http://www.bos.frb.org/commdev/c&b/1999/fall99.pdf . For reports of fears restricting the growth of electronic transactions *see* Dinesh C. Sharma, *Hacking fears bog down online banking growth*, CNET NEWS.COM, Sept. 6, 2005, http://news.com.com/2100-1038_3-5851061.html. (Polling shows that as many as 73% of American consumers are deterred from using online banking services); Dinesh C. Sharma, *Data leaks denting Web shoppers' confidence*, CNET NEWS.COM, June 23, 2005, http://news.com.com/2100-1029_3-5759294.html (one-third of online shoppers spending less than they would otherwise because of the fear of personal data theft); Robert Lemos, *Payroll firm pulls Web services, citing data leak*, CNET NEWS.COM, March 1, 2005, http://news.com.com/2100-1029_3-5595316.html (payroll firm ceasing its online services due to concerns about data theft).

20. Synovate, *Federal Trade Commission – Identity Theft Survey Report*, at 6 (2003), *available at* http://www.consumer.gov/idtheft/pdf/synovate_report.pdf .

21. The Fair Credit Reporting Act, 15 U.S.C. § 1681 (2006).

22. Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936 (1996).

23. Prohibition on release and use of certain personal information from state motor vehicle records, 18 U.S.C. §§ 2721-2725 (2006).

24. 15 U.S.C. §§ 1681a – 1681x.

25. 110 Stat. 1936.

26. Gramm-Leach-Bliley Act, 15 U.S.C. §§ 6801-6809 (2006).

27. The HIPAA and GLBA both rely on FTC enforcement

of their provisions, although the FCRA does provide an explicit private right of action. *See* §1177, 110 Stat. at 2029; 15 U.S.C. §6801; 15 U.S.C. §§ 1681n – 1681o.

28. For further analysis see Anthony D. Milewski Jr., *Compliance with California Privacy Laws: Federal Law Also Provides Guidance to Businesses Nationwide*, 2 Shidler J. L. Com. & Tech. 19 (2006), *available at* http://www.lctjournal.washington.edu/Vol2/a019Milewski.html .

29. Privacy Act of 1974, 5 U.S.C. § 552(a) (2006).

30. *Id.* Although the Federal Privacy Act only applies to federal agencies and private contractors as agents, several states have statutes analogous to the Privacy Act that apply to state agencies and political subdivisions.

31. *Id.*

32. Two Class Action Lawsuits have been filed based on the Privacy Act stemming from the release of the personal information of 26.5 million veterans and their families. *See* Anita Ramasastry, *Stolen Laptops and Data Theft: Why the Privacy Act Lawsuit against the Veteran's Administration May Succeed, and Why We Need Similar Remedies in the Private Sector*, FindLaw's Writ, June 15, 2006, http://writ.news.findlaw.com/ramasastry/20060615.html .

33. 5 U.S.C. § 552(a).

34. Thirty-five states and the federal government considered this type of legislation in 2005. As of January 1, 2006, twenty-three states had enacted laws requiring notification of individuals in the event of a security breach. *See* State PIRG Summary of State Security Freeze and Security Breach Notification Laws (2006), http://www.pirg.org/consumer/credit/statelaws.htm (last visited July 21, 2006).

35. For a complete discussion of the California Privacy law and its implications, *see* Milewski, *supra* note 28.

36. Cal. Civ. Code § 1798.29 (2006). The statute also provides an individual with a private cause of action. For more information regarding the California

notification requirements see John J. Altorelli & Michael K. Lindsey, *New California Law Requires Notification of Security Breaches Involving Personal Information*, 20 No. 10 Computer & Internet L. 10 (2003).

37. Cal. Civ. Code § 1798.81.5.

38. *See* Saul Ewing, *Technology Transactions and Intellectual Property; Pennsylvania, California Enact New Privacy Laws*, Feb. 2005, *available at* http://www.saul.com/common/publications/pdf_741.pdf .

39. Cal. Civ. Code § 1798.81.5 (2006).

40. Milewski, *supra* note 28.

41. Cal. Civ. Code § 1798.81.5(c).

42. Individually identifiable health information includes both demographic information (such as name, social security number, and address) and medical information. *See* Health Insurance Portability and Accountability Act, 42 U.S.C. § 1320(d)(6) (2006).

43. 45 C.F.R. § 164.306(a) (2006).

44. Of the 18 standards contained in HIPAA, nine are administrative, four are physical, and the remaining five are technical. The nine administrative standards focus on the steps an organization must take to manage their processes and employees. These safeguards range from implementing procedures to prevent and detect security intrusions, to training employees on the need for information security. The four physical standards focus on the physical security of the stored data. These standards include restricting access to areas with data by the use of locks, securing workstations that can access personal information, and implementing controls for the movement of workstation hardware. The five technical safeguards focus on procedures designed to protect the integrity of computer systems and other technology. These standards require implementation of procedures to: restrict access to approved users, regularly audit the information, protect the information from corruption, authenticate the user accessing the data, and protect the personal information in transmission. *See* 45 C.F.R. §§ 164.304-312 (2006); for a more complete list see *Information Security Program: Health Insurance*

Portability and Accountability Act (HIPAA) Compliance Guide, United States Department of Health and Human Services, Sept. 14, 2005, *available at* http://csrc.nist.gov/fasp/FASPDocs/program-mgmt/HHS_HIPAA_Compliance_Guide_09142005.pdf.

45. Milewski, *supra* note 28.

46. *Financial Institutions and Customer Information: Complying with the Safeguards Rule*, FTC FACTS for Business, Federal Trade Commission, Apr. 2006, *available at* http://www.ftc.gov/bcp/conline/pubs/buspubs/safeguards.htm .

47. The Safeguards Rule requires that covered organizations develop written security programs that address administrative, technical and physical safeguards. A security program must take the size and complexity of the organization as well as the sensitivity of the customer information. The plan must designate an employee to coordinate the security, identify risks to personal information, design and implement safeguards against those risks, ensuring service providers also take appropriate safeguards, and test and evaluate the implemented safeguards. The Plan should address risks to personal data in all areas, but especially in Employee Management and Training, Information Systems, and Detecting and Managing System Failures. *See* 16 C.F.R. §314.4 (2002); *Financial Institutions and Customer Information: Complying with the Safeguards Rule*, Federal Trade Commission, Apr. 2006, *available at* http://www.ftc.gov/bcp/conline/pubs/buspubs/safeguards .

48. Restatement (Second) of Torts § 314 (1965).

49. *See also* Restatement (Second) of Torts § 302B cmt. d (1965) ("[I]n the absence of any reason to expect the contrary, an actor may reasonably proceed upon the assumption that others will obey the criminal law."); Prosser & Keeton on The Law of Torts, 201 (W. Page Keeton, ed. 5th ed. 1984) (1941) (an actor may have a duty to protect the plaintiff if he "greatly increased the risk of harm to the plaintiff from the criminal acts of others.").

50. Prosser & Keeton on The Law of Torts, 203 (W. Page

Keeton, ed. 5th ed. 1984) (1941).

51. Remsburg v. Docusearch, Inc., 149 N.H. 148, 816 A.2d 1001 (2002).

52. *Id.* at 152-53.

53. *Id.* at 151

54. *Id.* at 154-55

55. *Id.*

56. *Remsburg,* 149 N.H. at 155, 816 A.2d at 1008.

57. Bell v. Mich. Council 25 of the Am. Fed'n of State, County, and Mun. Employees, 2005 WL 356306 (Mich. Ct. of App. 2005) (unpublished). *But see* Huggins v. Citibank, N.A., 355 S.C. 329, 333, 585 S.E.2d 275 (S.C. 2003) (certified question to the South Carolina Supreme Court from the U.S. District Court for the District of South Carolina holding that a bank that had issued credit cards in the name of a party to identity thieves was not negligent because there is no duty of care to non-customers, i.e. parties with whom no special relationship exists). For an in-depth discussion of the policy argument for imposing liability on those who use information for a business purpose, *see* Vincent R. Johnson & Alan Gunn, Studies in American Tort Law , 305-06 (3d ed. 2005). *See also*, 1 Modern Tort Law: Liability and Litigation § 3:14 (2d ed.) (listing other situations found to be lacking the requisite relationship to give rise to a duty).

58. *Bell*, 2005 WL 356306 at *5.

59. *Id.* at *1.

60. *Id.* at *5.

61. *Id.* at *1.

62. Remsburg v. Docusearch, Inc., 149 N.H. 148, 816 A.2d 1001 (2002); *Bell*, 2005 WL 356306 at *5.

63. *Remsburg*, 816 A.2d at 1006.

64. *Bell*, 2005 WL 356306 at *1.

65. Poli v. Mountain Valleys Health Ctrs, Inc., 2006 WL 83378 (E.D. Cal. 2006) (unpublished).

66. *Id*. at *1.

67. *Id.*

68. *Id*

69. *Id*. at *3.

70. *Id.*

71. *Id.*

72. Each jurisdiction provides its own formulation for determining when a duty exists, but in each jurisdiction the forseeability of the illegal act and harm is paramount. In *Bell* the Court considered the degree of certainty of the injury, the connection between the negligence and injury, and the burdens and costs of imposing a duty on the defendant. Bell v. Mich. Council 25 of the Am. Fed'n of State, County, and Mun. Employees, 2005 WL 356306 at *3 (Mich. Ct. of App. 2005) (unpublished).

73. RESTATEMENT (SECOND) OF TORTS § 302B cmt. d (1965).

74. *Id.* § 302B cmt. e(H) (1965).

75. Remsburg v. Docusearch, Inc., 816 A.2d 1001, 1008 (2002).

76. *Id.* at 1007-08.

77. Bell v. Mich. Council 25 of the Am. Fed'n of State, County, and Mun. Employees, 2005 WL 356306 at *5 (Mich. Ct. of App. 2005) (unpublished).

78. Jane Strachan, *Cybersecurity Obligations*, 20 Me. B. J. 90 (2005).

79. *In re* Verizon Related Reduction Claim, State of Maine Public Utilities Commission, Docket No. 2000-849 (April 30, 2003).

80. *Id.*

81. Cobell v. Norton, 391 F.3d 251 (DC Cir. 2004).

82. *Cobell v. Norton: an Overview*, INDIAN TRUST: COBELL V. KEMPTHORNE: http://www.indiantrust.com/index.cfm?FuseAction=Overview.Home (last visited July 21, 2006).

83. *Cobell*, 391 F.3d 251.

84. *See Financial Institutions and Customer Information: Complying with the Safeguards Rule*, Federal Trade Commission, Apr. 2006, *available at*

http://www.ftc.gov/bcp/conline/pubs/buspubs/safeguards.htm ; *Information Security Program: Health Insurance Portability and Accountability Act (HIPAA) Compliance Guide*, United States Department of Health and Human Services, Sept. 14, 2005 *available at* http://csrc.nist.gov/fasp/FASPDocs/program-mgmt/HHS_HIPAA_Compliance_Guide_09142005.pdf.

85. *See Financial Institutions and Customer Information: Complying with the Safeguards Rule*, *supra* note 34; *Information Security Program: Health Insurance Portability and Accountability Act (HIPAA) Compliance Guide*, *supra* note 34.

86. *See Financial Institutions and Customer Information: Complying with the Safeguards Rule*, *supra* note 34; *Information Security Program: Health Insurance Portability and Accountability Act (HIPAA) Compliance Guide*, *supra* note 34.

87. Bell v. Mich. Council 25 of the Am. Fed'n of State, County, and Mun. Employees, 2005 WL 356306 at *5 (Mich. Ct. of App. 2005)(unpublished).

88. Remsburg v. Docusearch, Inc., 816 A.2d 1001, 1008 (2002).

89. Cobell v. Norton, 391 F.3d 251 (DC Cir. 2004).

90. Vincent R. Johnson, *Cybersecurity, Identity Theft, and the Limits of Tort Liability*, 57 S.C. L. Rev. 255 (2005).

91. Strachan, *supra* note 75.

<< Top