CYBERSECURITY, IDENTITY THEFT, AND THE LIMITS OF TORT LIABILITY

Vincent R. Johnson*

I. The Vulnerable Foundations of Modern Society ..... Page 1

II. The Duty to Protect Database Information ..... Page 10
- **A. Statutes Legislatively Creating a Cause of Action** ..... Page 10
- **B. Statutes Judicially Determined to Set the Standard of Care** ..... Page 12
  - **1. The Gramm-Leach-Bliley Act** ..... Page 13
  - **2. State Security Breach Notification Laws** ..... Page 18
- **C. Basic Tort Principles** ..... Page 19
  - **1. *Palsgraf*, *Kline*, and Related Cases** ..... Page 19
  - **2. Public Policy Analysis** ..... Page 23
  - **3. Voluntary Assumption of Duty** ..... Page 25
- **D. Fiduciary Obligations** ..... Page 27

III. The Duty to Reveal Evidence of Security Breaches ..... Page 30
- **A. Statutory Duties** ..... Page 31
- **B. Basic Tort Principles** ..... Page 36
  - **1. General Duty or Limited Duty** ..... Page 36
  - **2. The Obligation to Correct Previous Statements** ..... Page 40
  - **3. Conduct Creating a Continuing Risk of Physical Harm** ..... Page 41
- **C. Fiduciary Duty of Candor** ..... Page 43

IV. Limiting Cybersecurity Tort Liability ..... Page 44
- **A. The Economic-Loss Rule** ..... Page 44
- **B. Emotional-Distress Damages** ..... Page 52
- **C. Security-Monitoring Damages** ..... Page 54

V. Conclusion: Security in Insecure Times ..... Page 60

I. The Vulnerable Foundations of Modern Society

In the developed world at the beginning of the 21st century, life is built upon

* Visiting Professor of Law, University of Notre Dame. Professor of Law, St. Mary's University, San Antonio, Texas. B.A., LL.D., St. Vincent College (Pa.); J.D. University of Notre Dame; LL.M., Yale University. Member, American Law Institute. Co-author, STUDIES IN AMERICAN TORT LAW (3d ed. 2005) (with Alan Gunn). Research and editorial assistance were provided by Graham D. Baker and Brenna Nava. Additional help was furnished by Claire G. Hargrove.

computerized databases. Those electronic troves contain a vast range of information about virtually all persons who interact (voluntarily or involuntarily) with the institutions of society. A myriad of entities, including businesses, non-profit organizations, and the government, assemble, update, manage, and use masses of computerized information relating to individuals.[1] The data often include, but certainly are not limited to, names, relationships (e.g., family members and employers), contact information (e.g., phone numbers, residences, and virtual addresses), personal histories (e.g., birth dates, medical data, physical characteristics, and educational records), official identifiers (e.g., social security, driver's license, and passport numbers), and financial records (e.g., bank, credit card, frequent flyer, and investment account numbers). Without such databases, virtually all types of enterprises would operate much less efficiently than they do today.

When information contained in computerized databases is hacked[2] or otherwise improperly accessed the consequences can be devastating for the persons to whom the information relates (data subjects). Among the more obvious risks is the possibility that an

---

[1] "Credit card transactions, magazine subscriptions, telephone numbers, real estate records, automobile registrations, consumer surveys, warranty registrations, credit reports, and Internet web sites are all sources of personal information . . . ." LA. REV. STAT. § 51:3072, La. Legis. 499 (2005) (legislative finding). "[B]usinesses and governments share everything from marketing lists to property records on the Internet." *Stop Thieves from Stealing You*, CONSUMER REPORTS, Oct. 2003, at 12 (hereinafter cited as "*Stop Thieves*").

[2] According to one source, "hacker" means "an unauthorized user who attempts to or gains access to an information system and the data it supports." Information Security Glossary Terms, at http://www.key.com/html/A-11.2.1.html#H (last visited July 24, 2005). *See also* Eric J. Sinrod & William P. Reilly, *Cyber-Crimes: A Practical Approach to the Application of Federal Computer Crime Laws*, 16 SANTA CLARA COMPUTER & HIGH TECH. L.J. 177, 182-88 (2000) (discussing "hackers" and "crackers"–the latter being hackers with criminal intent). In this article, unless context indicates otherwise, "hacker" means an "outside" unauthorized user. "One of the greatest threats to the security of client computers is not the hacker, but the enemy within: trusted company employees, ex-employees, consultants, or other insiders familiar with the computer network." Michael L. Rustad, *Private Enforcement of Cybercrime on the Electronic Frontier*, 11 S. CAL. INTERDISC. L.J. 63, 76 (2001). The term "data intruder" is used here to encompass both hackers and insiders without authorization to access data at the time or for the purposes that efforts to gain access are made.

State security breach notifications laws, discussed in Parts II-B-2 and III-A, have been passed to respond to the risks of harm caused by hackers and other intruders. Their application frequently pivots on a definition of "security breach." *See, e.g.,* CAL. CIV. CODE § 1798.82(d) (Westlaw current through Ch. 33 of 2005 Reg. Sess. urgency legislation & Gov. Reorg. Plan No. 2 of 2005) (defining a breach of security of a database as "unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the person or business"). The terms data intrusion and security breach are sometimes used synonymously here.

affected individual will become a victim of identity theft[3] and will suffer ruinous losses to credit and reputation, emotional distress, inconvenience, out-of-pocket expenses,[4] and perhaps even lost opportunities.[5] In more extreme cases, the individual to whom the information pertains may be stalked by an assailant, blackmailed,[6] or physically harmed.[7] The sources of unauthorized data access are diverse. "The perpetrators of computer intrusions may be bored juveniles, disgruntled employees, corporate spies, or organized crime networks,"[8] not to mention run-of-the-mill thieves.

News reports about hacking are now common.[9] Such breaches of data security often

---

[3] *See generally* Anthony E. White, *The Recognition of a Negligence Cause of Action for Victims of Identity Theft: Someone Stole My Identity, Now Who Is Going to Pay for It?*, 88 MARQ. L. REV. 847, 851-52 (2005) (discussing "account takeovers" and "true name fraud"); R. Bradley McMahon, *After Billions Spent to Comply with HIPAA and GLBA Privacy Provisions, Why Is Identity Theft the Most Prevalent Crime in America?*, 49 Vill. L. Rev. 625, 627 (2004) (discussing how identity theft occurs); *see also* FEDERAL TRADE COMMISSION, FEDERAL AND STATE TRENDS IN FRAUD AND IDENTITY THEFT JANUARY TO DECEMBER, 2004 (2005), *available at* http://www.consumer.gov/sentinel/pubs/Top10Fraud2004.pdf (last visited July 25, 2005) (gathering statistics).

[4] Texas Bill Analysis, 2005 Reg. Sess. Sen. Bill 122, *available in Westlaw at* Tx. B. An., S.B. 122, 4/7/2005 (reporting that "[v]ictims spend an average of 600 hours over two to four years and $1,400 to clear their names").

[5] *Identity Theft* at http://www.consumer.gov/idtheft (stating that as a result of identity theft "victims may lose job opportunities, be refused loans, education, housing or cars, or even get arrested for crimes they didn't commit") (hereinafter "FTC website"). For example, a hacker may be able to access an admissions application, change the data submitted online, and thereby reduce the applicant's chances of being accepted. *Cf.* Robert Lemos, *USC admissions site cracked wide open*, THE REGISTER, July 7, 2005, *available at* http://www.theregister.co.uk/2005/07/06/usc_site_cracked (last visited July 8, 2005) (discussing a flaw in a university application system that "left the personal information of users publicly accessible").

[6] *Cf.* Rustad, , *supra* note 2, 6, at 100 (reporting that "[a] former chemistry graduate student found a security flaw in a commercial website and demanded ransom payments to keep quiet about it").

[7] *Cf.* Remsburg v. Docusearch, Inc., 816 A.2d 1001 (N.H. 2003). *Remsburg* is discussed in the text beginning at note 233.

[8] *See* Rustad, *supra* note 2, 6, at 65.

[9] *See, e.g.*, *University to Warn Web Users of Security Breach by Hackers*, N.Y. TIMES, July 10, 2005, at 15, col. 1 (discussing plans by the University of Southern California to notify 270,000 persons that hacking occurred).; John C. Ensslin, *2 CU Computers Hacked*, ROCKY MT. NEWS, July 22, 2005, *available at* http://www.rockymountainnews.com/drmn/education/article/0,1299,DRMN_957_3945801,00.html (discussing security breaches at the University of Colorado that exposed the personal data of 42,900 students, faculty, and staff members). *See also* DELOITTE, 2004 GLOBAL SECURITY SURVEY 24 (2004), available at http://dtt_financialservices_SecuritySurvey2004_051704.pdf

threaten the interests of hundreds or thousands of persons simultaneously.[10] Because database use is ubiquitous, virtually everyone is a potential victim.[11]

(last visited Aug 2, 2004) (reporting that a survey of major global financial institutions revealed that 83% reported a breach of computer security during the last year, and that while "outside intrusions were more common from those on the inside," the majority of respondents experienced both).

[10] *Cf.* Eric Dash, *Europe Zips Lips; U.S. Sells Zips*, N.Y. TIMES, Sun. Aug. 7, 2005, at sec. 4, p.1. (stating that in 2005, "the personal information of more than 50 million consumers has been lost, stolen and even sold to thieves"); Eric Dash, *Credit Card Ads Place Renewed Focus on Security*, N.Y. TIMES, July 18, 2005 (indicating that Bank of America reported in February 2005 that it had lost data tapes containing millions of its customers' records"); Lemos, *supra* note 5, (discussing a flaw in an online university application system that "put at risk 'hundreds of thousands' of records containing personal information"); Melissa Sanchez, *Breach Exposes School Records*, FT. WORTH STAR-TELEGRAM, Tues. Aug. 9, 2005 (discussing a breach of security at the University of North Texas which compromised data relating to more than 38,000 present, former, and prospective students); Calif. Bill Analysis, Senate Floor, 2001-2002 Regular Session, Assembly Bill 700, Aug. 22, 2002, *available in* Westlaw at CA B. An., A.B. 700 Sen., 8/22/2002 (reporting that "computer hackers were able to illegally access sensitive financial and personal information, including Social Security numbers, of approximately 265,000 state workers").

[11] *See* David B. Reddick, National Assoc. of Mut. Ins. Cos., *Security Breach Notification Laws*, 1 ISSUE BRIEF No. 3, at 2 (Jul. 7, 2005) (indicating that during a recent year more than 10 million persons were victims of identity theft, which "topped the FTC's annual complaints list for the fifth year in a row"), *available at* http://www.namic.org/insbriefs/050707SecurityBreach.pdf.

Hackers and other data intruders are subject to criminal[12] and civil liability.[13] They can be sued, sometimes successfully,[14] under a variety of tort theories, including conversion,[15] trespass to chattels,[16] and intrusion upon private affairs,[17] as well as under the civil liability

---

[12] *See* Jason Krause, *The Case of the Ethical Hacker*, 2 No. 44 A.B.A. J. E-REPORT 2 (Nov. 2003), *available in* Westlaw at 2 No. 44 ABAJEREP 2 (discussing criminal liability under the federal Computer Fraud and Abuse Act); Current Development, *Federal Jury Convicts Smart-Card Hacker for Violating DMCA*, 20 No. 12 INTERNET & COMPUTER LAW. 28 (2003) (discussing the first hacker conviction under the Digital Millennium Copyright Act). *See also* CRITICAL INFORMATION INFRASTRUCTURE PROTECTION AND THE LAW: AN OVERVIEW OF KEY ISSUES 37-39 (Stewart D. Personick *et al*. eds., 2003), at http://books.nap.edu/html/ciip/index.html [hereinafter CRITICAL INFORMATION INFRASTRUCTURE] (briefly discussing the federal Computer Fraud and Abuse Act, the Electronic Communications Privacy Act, and the USA Patriot Act, as well as fraud in connection with "access devices" and interception of communications); Brent Wibel, *A Site Where Hackers Are Welcome: Using Hack-in Contests to Shape Preferences and Deter Computer Crime*, 112 YALE L.J. 1577 (2003) (discussing computer crime involving unwarranted intrusions into private computer networks). Hackers who misuse improperly accessed personal information may also be subject to liability under the identity-theft laws. *See* White, *supra* note 3, at 856 (indicating that 44 states have identity-theft statutes and that, in 1998, Congress passed the Identity Theft and Deterrence Act).

[13] *See* Rustad, *supra* note 2, 6, at 66 (predicting that "[t]ort remedies . . . will play an increasingly important role in punishing and deterring fraud, hacking, and other wrongdoing on the Internet").

[14] *See* Michael L. Rustad & Thomas H. Koenig, *Cybertorts and Legal Lag: an Empirical Analysis*, 13 S. CAL. INTERDISC. L.J. 77, 85 (2003) (stating that "[h]ardly a day goes by without new media reports of cyberspace wrongs, yet plaintiff victories remain rare"). Whether there is something to be said on behalf of hackers to mitigate or avoid liability is a subject of debate. According to "the main principles of hacking . . . information should circulate as widely as possible." Nicholas Thompson, *Who Needs Keys? Hackers Learn How to Trespass the Old-Fashioned Way—From a Lockpicker*, 2004-Dec. LEGAL AFF. 8. *See also* Krause, *supra* note 12, at 2 (stating that "[o]ne of the activities that defines the hacker community is the process of looking for software security holes and publishing details of security flaws on the Web. . . . Some argue this research is a kind of peer review that is vital to computer science"); Wibel, *supra* note 12, at 1589-92 (discussing the transformation of hacker culture and stressing the need to "rebuild a community of hackers in which a body of positive social norms can be sustained").

[15] *See* Rustad, *supra* note 2, 6, at 114 (opining that "a virus that destroys a hard drive might be conceptualized as the tort of conversion").

[16] *See id.* at 106 (stating that "[c]ourts have held that a hacker's intrusion into a computer network constitutes a trespass to chattels").

[17] *See* Shannon Duffy, *Law Firm Accused of Hacking*, THE LEGAL INTELLIGENCER, July 14, 2005, at http://www.law.com/jsp/ltn/pubArticleLTN.jsp?id=1121245509109 (last visited July 19, 2005) (discussing a suit against a law firm for copyright infringement, civil conspiracy, trespass to chattels, trespass for conversion and intrusion upon seclusion).

provisions of the federal Computer Fraud & Abuse Act.[18] However, hackers (particularly those located in other countries[19]) may be difficult to identify or subject to court jurisdiction. Hackers may also be judgment proof.[20] A better target for a lawsuit–one easier to locate, more amenable to legal process, and perhaps more solvent–may be the database possessor[21] who failed to

---

[18] 18 U.S.C. § 1030(g) (Westlaw current through P.L. 109-18, approved June 29, 2005) (stating in part that "[a]ny person who suffers damage . . . may maintain a civil action against the violator to obtain compensatory damages and injunctive relief or other equitable relief"). *See generally* Rustad, *supra* note 2, 6, at 89-91 (describing the CFFA).

[19] *See* Ensslin, *supra* note 9 (discussing attacks traced to France and Eastern Europe); Rustad, *supra* note 2, 6, at 74 (stating that the "Russian Republics have been a popular venue for innovative cyberscams involving credit card numbers stolen from websites"); Calif. Bill Analysis, Senate Floor, 2001-2002 Regular Session, Assembly Bill 700, Aug. 22, 2002, *available in* Westlaw at CA B. An., A.B. 700 Sen., 8/22/2002 (discussing use of hacked data by "unauthorized persons in Germany").

[20] *See* Wibel, *supra* note 12, at 1582 (asserting that "hackers tend to be judgment proof").

[21] There is an important initial terminological question relating cybersecurity tort liability: if there is to be a duty of care and a risk of liability, on whom should the duty and risk be imposed? Should the analysis focus on the obligations of database owners, or database possessors, or some other class of persons? This article speaks in terms of the duty and liability of database "possessors," on the assumption that a party in possession of the data has the opportunity to exercise care. The term would include owners or licensees in possession of data and perhaps others. The choice to focus on possession of data finds analogical support in the law of premises liability, which generally imposes duties and liability on the party in possession of the premises at the time the harm occurred. (For example, a lessor not in possession of a leased premises, in many states, is subject to only limited liability. *See, e.g.*, Clauson v. Kempffer, 477 N.W.2d 257 (S.D. 1991) (holding that a landlord had no duty to warn a motorcyclist of a smooth wire fence that tenants strung across a road on a leased premises).) However, a legislature or court might elect to speak in other terms. State security breach notification statutes generally only require data owners or licensors to notify data subjects that unauthorized access to data has occurred. *See, e.g.*, CAL. CIV. CODE § 1798.81.5 (Westlaw current through Ch. 33 of 2005 Reg. Sess. urgency legislation & Gov. Reorg. Plan No. 2 of 2005) (imposing obligations on a "business that owns to licenses personal information"); 2005 TENN. LAWS PUB. CH. 473 §§ 1(a)(2) & (b) (S.B. 2220), Tn. Legis. 473 (2005) (imposing obligations on an "information holder," which is defined as a business or state agency that "that owns or licenses computerized data that includes personal information"). State security breach notification laws generally oblige database possessors who do not own the data that has been breached to disclose the intrusion to the owner of the data, rather than the data subject. See CAL. CIV. CODE § 1798.82(b) (Westlaw current through Ch. 33 of 2005 Reg. Sess. urgency legislation & Gov. Reorg. Plan No. 2 of 2005) (imposing obligations on a "business that owns to licenses personal information") (stating that "[a]ny person or business that maintains computerized data that includes personal information that the person or business does not own shall notify the owner or licensee of the information of any breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized

prevent or reveal the security breach, rather than the intruder.

Whether and to what extent a database possessor can be held liable for damages suffered by data subjects as a result of improper data access are questions of huge importance. On one hand, unless some form of liability is imposed, the persons often in the best position to prevent the losses may have insufficient incentive to exercise care to avoid unnecessary harm. On the other hand, if liability is too readily assessed, it will have the power to bankrupt valuable enterprises because of the often vast numbers of potential plaintiffs and consequent extensive resulting damages.[22] Obviously, a balance must be struck that adequately protects the interests of individuals without discouraging the use of computer technology or driving important institutions out of existence.

Cases are now being litigated over the liability of database possessors,[23] and lawyers are starting to advise clients about the risk of being held accountable for harm caused by hackers and other intruders.[24] However, despite the recent enactment of security breach notification statutes in at least fifteen states,[25] the law governing database possessor liability is far from settled.

---

person").

[22] *See* Robert Steinberg, *Advising Clients About Hacker Insurance*, L.A. LAW., Feb. 2003, at 60, *available in* Westlaw at 25-Feb. L.A. Law. 60 (opining that "[f]or corporations with well-known brand names, in high visibility industries, with significant Web presences, or sensitive information, a single breach, with the potential for third-party claims, can be financially devastating"). *See also* Ethan Preston & Paul Turner, *The Global Rise of a Duty to Disclose Information Security Breaches*, 22 J. MARSHALL J. COMPUTER & INFO. L. 457, 491 (2004) (reporting that "[o]ne study found that publicly-traded firms which disclosed security breaches lost 2.1% of their market value within two days of the disclosure").

[23] *See, e.g.*, Parke v. Cardsystems Solutions, Inc., No. CGC - 05 - 442624 (CA. Super Ct. filed June 24, 2005) (alleging, in a class action, that information relating to 40 million credit card accounts was accessed by hackers and that the defendants had failed to protect the data or promptly notify data subjects about the breach); Goldberg v. ChoicePoint Inc., No. BC329115 (Cal. Super. Ct. filed Feb. 18, 2005) (alleging, in a class action involving 145,000 persons, that the defendants failed to protect personal data, failed to promptly notify data subjects of the breach, engaged in unfair business practices, and committed fraud and negligent misrepresentation). *See also* Laura Mahoney, *Identity Theft Class Action Filed Against ChoicePoint as AG Launches Investigation into Breach*, 6 COMPUTER TECH. L. REP. Mar. 4, 2005 (indicating that the state was "tracking about 4 cases that have been significant in size").

[24] *See* Jane Strachan, *Cybersecurity Obligations*, 20 ME. B.J. 90 (2005) (discussing how to advise business clients in light of "[t]oday's. . . risk of a lawsuit or regulatory enforcement arising from inadequate information security practices").

[25] *See* ARK. CODE ANN. § 4-110-101, *et seq*., Ar. Legis. 1526 (2005); CAL. CIV. CODE § 1798.81.5 *et seq.* (Westlaw current through Ch. 33 of 2005 Reg. Sess. urgency legislation & Gov. Reorg. Plan No. 2 of 2005); 2005 CONN. LEGIS. SERV. P.A. 05-148 (S.S.B. 650), Ct. Legis. P.A. 05-148; DEL. CODE ANN. tit. 6, § 12B-101 *et seq*., De. Legis. 61 (2005); FLA. STAT. ANN. § 817.5681 *et seq.*, Fl. Legis. 2005-229; GA. CODE ANN. § 10-1-910 *et seq*., Ga. Legis. 163 (2005); 815 ILL. COMP. STAT. § 530/1 *et seq.*, Il. Legis. 94-36 (2005); IND. CODE § 4-1-11-1 *et seq.*, In.

There is considerable uncertainty about the reach of the new state laws and related concerns, including what types of damages might be recovered in tort actions involving data intrusion. This article addresses three key questions relating to database possessor liability for harm caused by data intruders.[26]

The first issue, considered in Part II, is whether database possessors have a legal duty to data subjects to safeguard their personal information from unauthorized access by hackers or others. The discussion addresses the obligations imposed by statutes, ordinary tort principles (including the rules on voluntary assumption of duty), and fiduciary-duty law. The article concludes that, in a wide range of circumstances, database possessors are (or should be) legally obliged to data subjects to exercise reasonable care to safeguard personal data from intruders. However, as discussed below, the precise theory under which such a duty is imposed may have important implications for defining the scope of liability.

Legis. 91-2005 (2005); LA. REV. STAT. § 51:3071 *et seq*., La. Legis. 499 (2005); ME. REV. STAT. § 1346 *et seq*., Me. Legis. 379 (2005); MINN. STAT. § 325E.61 *et seq*., Mn. Legis. 167 (2005); MONT. CODE ANN. § 31-3-115(5), Mt. Legis. 518 (2005); 2005 NEV. LAWS Ch. 486 (A.B. 334), §§ 4 & 6, Nv. Legis. 486 (2005) (slip copy) and 2005 Nevada Laws Ch. 485 (S.B. 347), § 17 *et seq.*, Nv. Legis. 485 (2005) (slip copy); N.D. CENT. CODE § 51-30-01 *et seq*., N.D. Legis. 447 (2005); R.I. GEN. LAWS. § 11-49.2-1 *et seq.*, R.I. Legis. 05-225; 2005 TENN. LAWS PUB. CH. 473 (S.B. 2220), Tn. Legis. 473 (2005); TEX. BUS. & COM. CODE § 48.001 *et seq.*, Tx. Legis. 294 (2005); WASH. REV. CODE § 42.17 *et seq.*, Wa. Legis. 368 (2005). *See generally* Reddick, *supra* note 4, at 1-5 (analyzing security breach notification laws for an insurance trade association).

[26] A database possessor may "lose" the personal information of others in a variety of ways: for example, (1) by failing to protect the information from hackers and other intruders; (2) by erroneously releasing the information to third persons; or (3) by simply misplacing the data. In one sense, these three forms of data loss each involve alleged failure to exercise reasonable case, and in that respect may be nothing more than different examples of negligent data handling. However, on closer scrutiny, the three types of data loss identified above may be legally distinguishable. Failure to guard against intruders raises the issue of whether there is a duty to undertake what amounts to crime fighting efforts–which is a point of some controversy. *See* Dupont v. Aavid Thermal Tech., Inc., 798 A.2d 587, 592 (N.H. 2002) (holding that there is no broad duty on an employer to protect an employee from foreseeable crimes because "the general duty to protect citizens from criminal attacks is a government function"). In contrast, the duty to protect third persons from criminal intruders is not a significant concern in cases involving erroneous release or careless loss of data. Similarly, when the wrong data has been published erroneously, there has been an exercise (albeit an imprudent exercise) of first amendment rights to free speech or free press. The constitutional principles that have evolved to constrain the imposition of tort liability for utterances resulting in defamation or incitement might arguably also limit the levying of tort liability for erroneous publication of data that causes harm. However, those same principles would have no application in suits involving hacked or misplaced data, because in those situations there was never an intent on the part of the database possessor to speak or publish anything. Tort literature has not yet fully explored the issues relating to these various types of data loss. This article is primarily concerned with a database possessor's duty to protect data from intruders.

The next issue, considered in Part III, concerns not whether there is a duty *to protect* computerized information from intruders, but whether a database possessor is obliged *to disclose* evidence of a security breach to data subjects once an intrusion occurs. The discussion considers statutory obligations, as well as basic tort principles. The relevant legislation includes the security breach notification laws recently passed in many states. Pertinent common-law guidance encompasses the basic principles of negligence liability and two specific rules that warrant special attention. The first rule, under the law of misrepresentation, imposes a duty to update previously accurate statements that are the basis for pending or continuing reliance.[27] This rule is relevant because a breach of data security may cast substantial doubt on the continuing accuracy of expansive statements about data security that are often contained in business advertisements or published privacy policies. The second rule, under failure-to-act jurisprudence, creates a duty to exercise reasonable care to prevent harm or minimize adverse consequences if one's prior conduct, "even though not tortious," creates a continuing risk of physical harm.[28] This rule may be relevant because the security practices of database possessors, even if not negligent, often contribute to the success of hackers and other intruders. Finally, the heightened candor obligations imposed by fiduciary-duty law are considered. The article concludes that in many situations there is (or should be) a duty, enforceable in a tort action for damages, to inform data subjects that the security of their data has been compromised.

The final key issue, addressed in Part IV, concerns how far the liability of a database possessor should extend in cases where the possessor has failed to exercise reasonable care to protect data or disclose information about intrusion. The discussion first considers the economic-loss rule[29] and concludes that it presents an important, but limited, obstacle to recovery of tort damages. Under certain circumstances, economic damages caused by identity theft resulting from improperly accessed data should be recoverable The article then addresses the issue of emotional distress damages and considers the arguments favoring limited liability for this type of loss in cybersecurity litigation. Attention is paid to the guidance that has emerged from the courts in fear-of-disease cases, and the article recommends adapting those principles to the context of improperly accessed data. Emotional-distress damages should be available only to those plaintiffs whose data was actually accessed by an intruder, and not to those whose data was merely exposed to a risk of unauthorized access. Lastly, the article argues that, in the absence of aggravated tortious conduct (e.g., recklessness or worse), the interests of

---

[27] *See, e g.*, McGrath v. Zenith Radio Corp., 651 F.2d 458, 468 (7th Cir. 1981) (holding that the failure to correct earlier true statements, which has become false or misleading, was fraudulent).

[28] *See* RESTATEMENT, THIRD, OF TORTS: LIABILITY FOR PHYSICAL HARM § 39 (Proposed Final Draft No. 1, 2005) (discussing duty based on prior conduct).

[29] *See generally* Jay M. Feinman, *Doctrinal Classification and Economic Negligence*, 33 SAN DIEGO L. REV. 137, 146 (1996) (stating that "the economic loss rule distinguishes purely pecuniary losses from losses due to personal injury or property damage losses as the criterion that governs the classification of cases. Economic losses are losses due to disappointed expectations, and should therefore be governed by contract law; only losses due to personal injury or property damage, which generally are not the subject of prior bargaining and which invoke public safety concerns, are within the realm of tort law").

society will be best served by limiting recoverable losses to the cost of "security-monitoring" damages once a database possessor discloses to the affected individual the fact that data has been improperly accessed. This approach will encourage database possessors to discover and reveal instances of data intrusion. It will also place data subjects in a position to protect their own interests by monitoring their economic and personal security when there is heightened vulnerability. This proposal relating to security-monitoring damages is similar in concept to medical-monitoring damages,[30] a type of loss that many states permit victims of toxic exposure to recover. The proposed limitation on liability will encourage the exercise of care by both database possessors and data subjects, while at the same time minimizing the risk of imposing the type of extensive tort damages that would discourage the use of computer technology or assess disproportionate liability.

II. The Duty to Protect Database Information

Tort liability depends upon the existence of a legal duty to exercise care running from the defendant (the database possessor) to the plaintiff (the data subject). Such a duty may be imposed either by statute or by common law. The following sections discuss legislation bearing on the question of whether there is a tort duty to safeguard the security of computerized personal data and two obvious sources of common-law guidance, ordinary tort principles and fiduciary-duty law.

A. Statutes Legislatively Creating a Cause of Action

A duty to exercise care to protect data from intruders may be imposed by statute,[31] either by the express terms of the legislation[32] or because a court holds that a statute that is silent as to civil liability sets the appropriate standard of care for a tort action.[33] This subpart discusses

---

[30] "In the context of a toxic exposure action, a claim for medical monitoring seeks to recover the cost of future periodic medical examinations intended to facilitate early detection and treatment of disease caused by a plaintiff's exposure to toxic substances." Potter v. Firestone Tire and Rubber Co., 863 P.2d 795, 821 (Cal. 1993). *See also* Badillo v. American Brands, Inc., 16 P.3d 435, 439 (Nev. 2001) (noting that "a growing number of appellate courts have recognized medical monitoring (seventeen states plus the District of Columbia)").

[31] *See* Rustad, *supra* note 2, 6, at 108 (stating that "[a] hospital has a statutory duty to protect the privacy of its patients' records").

[32] *See* RESTATEMENT, THIRD, OF TORTS: LIABILITY FOR PHYSICAL HARM § 14 cmt. b (Proposed Final Draft No. 1) (discussing express and implied statutory causes of action).

[33] Sometimes courts find that there is an "implicit" legislative intent to create a civil cause of action; other times they simply hold that the statute is an appropriate expression of the standard of care. *See* VINCENT R. JOHNSON & ALAN GUNN, STUDIES IN AMERICAN TORT LAW 305-06 (3d ed. 2005) (stating that "[i]n the one case, the court is saying that the legislation sets the standard because the legislature implicitly intended it to do so, and in the other case, the court acknowledges that the statutes sets the standard because the court thinks that is a good idea. Either way, if the statute does not expressly create a cause of action, the essential inquiry is the same: was the law intended to protect this class of persons from this type of harm").

statutes that expressly create a civil cause of action based on lack of data security. The next subpart discusses statutes which do not create a tort cause of action, but might be judicially embraced as setting the standard of care for suits involving allegedly negligent failure to safeguard computerized personal data.

An important example of legislation expressly creating a civil cause of action for failure to protect data is California's much-discussed[34] Security Breach Information Act (SBIA). The SBIA was the first law in the United States to impose on businesses a duty to inform data subjects of unauthorized intrusion into their personal data.[35] The California act has served as a model for legislation subsequently adopted in other jurisdictions.[36] The various state laws are animated by mutual concerns and often share a common language and structure. The laws all impose a duty to reveal information about security breaches.[37] However, the statutes differ in important respects. One key difference concerns whether the statutes expressly impose a duty to protect data (in addition to the notification duty). Another key difference is whether a breach of the duties imposed by the act is expressly actionable in a private lawsuit.

The California SBIA imposes a data protection obligation and expressly authorizes maintenance of a suit for damages for breach of that duty. The relevant language, which became effective July 1, 2003,[38] states that:

> (b) A business that owns or licenses personal information about a California resident shall 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.[39]

The legislation further provides that:

> (b) Any customer injured by a violation of this title may institute a civil action to

---

[34] *See, e.g.*, Preston & Turner, *supra* note page 7, at 461-63.

[35] *See* Reddick, *supra* note 11, at 2 (stating point).

[36] *See* Reddick, *supra* note 11, at 1 (indicating that "most new laws follow the SBIA").

[37] *See* Part III-A (discussing notification laws).

[38] *See* Daniel J. McCoy, *Recent Privacy Law Developments Affecting the Workplace*, 788 PLI/PAT 435, 489 (May 2004) (discussing the California law).

[39] CAL. CIV. CODE § 1798.81.5 (Westlaw current through Ch. 33 of 2005 Reg. Sess. urgency legislation & Gov. Reorg. Plan No. 2 of 2005). The term "business" is defined broadly by the statute. *See id*. at § 1798.80(a). However, § 1798.81.5 does not apply to certain specified entities, including, among others, certain health care providers and financial institutions. *See id.* at § 1798.81.5(e). The obligations imposed by the California statute reach "well beyond California's borders, potentially affecting any company, person or agency that has a computer database containing any California resident's 'personal information.'" Tyler Paetkau & Roxanne Torabian-Bashardoust, *California Deals with ID Theft*, 13-Jun. BUS. L. TODAY 37 (2004). Importantly, "the law only applies when an individual's 'unencrypted data' is at issue." *Id.* at 41.

recover damages.[40]

The SBIA leaves no doubt that businesses owe a legal duty to customers under California law to protect their personal information, and that, if the duty is breached, damages may be recovered. It is also clear that the civil actions which the California legislature has told the courts to entertain are rooted in principles of negligence (rather than, for example, strict liability or recklessness), for the law speaks of "*reasonable* security procedures and practices"[41] that are "appropriate to the nature of the information."[42] Reasonableness assessed under the circumstances is the essence of the negligence standard of care. Only *unreasonable* (*i.e.*, negligent) conduct violates the California SBIA. However, beyond offering clear guidance regarding the existence of duty and the liability regime,[43] the SBIA leaves many matters unsettled. The act makes no attempt to define what constitutes "reasonable security procedures and practices." Presumably that assessment is left to the finder of fact for determination on a case by case basis. More importantly, the SBIA gives no indication as to what types of damages are recoverable.[44] Whether those damages include compensation for personal injury, property damage, emotional distress, economic loss, or other types of harm is left unresolved. If the legislature intended for courts to allow recovery of the "usual" types of damages that may be awarded in negligence suits, the scope of damages, as discussed in Part IV, may be more limited than might first appear.

B. Statutes Judicially Determined to Set the Standard of Care

Some statutes addressing issues relating to data protection do not expressly create a civil cause of action. In this category are the federal Gramm-Leach-Bliley Financial Modernization

---

[40] CAL. CIV. CODE § 1798.84 (Westlaw current through Ch. 33 of 2005 Reg. Sess. urgency legislation & Gov. Reorg. Plan No. 2 of 2005).

[41] *Id.* at § 1798.81.5.

[42] *Id.*

[43] The fact that liability is rooted in negligence may mean that an action is subject to a comparative negligence defense. *See* RESTATEMENT, THIRD, OF TORTS: LIABILITY FOR PHYSICAL HARM § 14 cmt. b (Proposed Final Draft No. 1, 2005) (stating that in dealing with a liability right expressly created by a statute, "the court may need to consider whether traditional tort defenses such as comparative negligence should be deemed impliedly incorporated into the statutory cause of action). *But see* Seim v. Garavalia, 306 N.W.2d 806, 811-13 (Minn. 1981) (discussing situations where statutes impose "absolute" liability).

[44] While adoption of the SBIA was pending, the Information Technology Association of America (ITAA) wrote to the state Senate Committee on Privacy and raised the "specter of lawsuits targeting companies for even innocent mistakes" and requested amendments to "cap the liability exposure." Calif. Bill Analysis, Senate Floor, 2001-2002 Regular Session, Assembly Bill 700, Aug. 22, 2002, *available in* Westlaw at CA B. An., A.B. 700 Sen., 8/22/2002. However, the ITAA offered no suggestion for how to effectuate such a cap, and the Committee report simply notes that "AB 700 does not create any new penalty in law." *Id.*

Act of 1999[45] ("GLBA") and certain state security breach notification laws. These various pieces of legislation are discussed in the following subparts.

1. The Gramm-Leach-Bliley Act

The GLBA states that it is "the policy of the Congress that each financial institution has *an affirmative and continuing obligation* to respect the privacy of its customers and *to protect the security and confidentiality of those customers' nonpublic personal information.*"[46] In furtherance of that policy, a significant number of state and federal governmental entities[47] are required to establish[48] and enforce[49] "appropriate standards for the financial institutions[50] subject to their jurisdiction."[51] Those standards must provide "administrative, technical, and physical safeguards–(1) to insure the security and confidentiality of customer records and information; (2) to protect against any anticipated threats or hazards to the security or integrity of such records; and (3) to protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer."[52]

The GLBA does not expressly create a civil cause of action against financial institutions for breach of their duty to protect customer information.[53] However, it has been suggested[54] that

---

[45] Gramm-Leach-Bliley Act of 1999, Pub. L. No. 106-102, 113 Stat. 1338 (1999) (codified in scattered sections of 12 and 15 U.S.C.).

[46] Gramm-Leach-Bliley Act of 1999, 15 U.S.C. 6801(a) (Westlaw current through P.L. 109-34, approved July 12, 2005) (emphasis added).

[47] *Id.* at 15 U.S.C. 6805 (defining entities and roles). *See also* id. at 15 U.S.C.A. § 6825 (stating that each Federal banking agency . . . , the National Credit Union Administration, and the Securities and Exchange Commission or self-regulatory organizations, as appropriate, shall review regulations and guidelines applicable to financial institutions under their respective jurisdictions and shall prescribe such revisions to such regulations and guidelines as may be necessary to ensure that such financial institutions have policies, procedures, and controls in place to prevent the unauthorized disclosure of customer financial information and to deter and detect . . . [the solicitation or obtaining of customer information by false pretenses]").

[48] *Id.* at 15 U.S.C. 6801(b) (discussing establishment of regulations).

[49] *Id.* at 15 U.S.C. 6805(a) (providing that regulations shall be "enforced by the Federal functional regulators, the State insurance authorities, and the Federal Trade Commission with respect to financial institutions and other persons subject to their jurisdiction").

[50] "Financial institutions under the Act include everything from real estate appraisers to automobile dealerships." McMahon, *supra* note 3, at 634-35.

[51] Gramm-Leach-Bliley Act of 1999, 15 U.S.C. 6801(b) (Westlaw current through P.L. 109-34, approved July 12, 2005) .

[52] *Id.* (emphasis added).

[53] Julia C. Schiller, Comment, *Informational Privacy v. The Commercial Speech Doctrine: Can the Gramm-Leach-Bliley Act Provide Adequate Privacy Protection?*, 11 COMMLAW CONSPECTUS 349, 356 (2003) (stating that "[t]he GLB Act . . . does not provide for a private right of action for consumers to sue the financial institution directly for violation of the statute"). "The consumer must complain to the agency having jurisdiction over them and that

the provisions of the act, or the standards adopted pursuant to the act, might serve as the predicate for a tort action on what is sometimes called a "negligence *per se"* theory.[55]

Under negligence *per se*, a court may, in its discretion, embrace a statute that does not expressly provide for a civil cause of action as the standard of care for a tort suit. If the enactment was intended to protect the class of persons of which the plaintiff is a member from the type of harm that occurred, a court may determine that violation of the statute defines the appropriate terms for imposing civil liability.[56] For example, courts have frequently adopted traffic rules[57]–requiring drivers to travel in the proper lane,[58] use headlights after dark,[59] or not exceed the speed limit[60]–as setting the standard of care in auto accident cases because those laws were intended to protect others on the road from the risk of physical harm. Referring to such legislative enactments in tort litigation serves the "function of simplifying or providing structure to the rendering of negligence determinations."[61] It also helps to ensure consistency in the resolution of issues of recurring importance and provides clear notice to others as to what should

---

agency may bring a court action against the financial institution. However, some state laws, such as the Unfair and Deceptive Practice Laws, may enable the consumer to claim that a violation of the GLBA violated other rights granted to the individual by the state." *Id.*

[54] *See* White, *supra* note footnote 3, at 865 (discussing negligence per se under the GLBA).

[55] *See generally* RESTATEMENT, THIRD, OF TORTS: LIABILITY FOR PHYSICAL HARM § 14 (Proposed Final Draft No. 1, 2005) (discussing negligence *per se*). In most jurisdictions, the unexcused violation of a standard-setting statute is conclusive proof of breach of duty, called negligence *per se* (*see generally* RESTATEMENT, THIRD, OF TORTS: LIABILITY FOR PHYSICAL HARM § 14 cmt. c (Proposed Final Draft No. 1, 2005)) or *prima facie* negligence (*see, e.g.*, Transportation Dept. v. Christensen, 581 N.W.2d 807, 809 (Mich. App. 1998). Regardless of the precise procedural effect of establishing an unexcused violation, in these states the determination that the enactment is controlling answers in the affirmative the question of whether there is a legal duty running from the defendant to the plaintiff. The jury is not free to ignore that determination. *See* Martin v. Herzog, 126 N.E. 814, 815 (N.Y. 1920) (stating that "[j]urors have no dispensing power").

[56] *See generally* RESTATEMENT, THIRD, OF TORTS: LIABILITY FOR PHYSICAL HARM § 14 (Proposed Final Draft No. 1, 2005) (discussing relevant considerations).

[57] *See* RESTATEMENT, THIRD, OF TORTS: LIABILITY FOR PHYSICAL HARM § 14 cmt. d (Proposed Final Draft No. 1, 2005) (noting that "in most highway-accident cases, findings of negligence depend on ascertaining which party has violated the relevant provisions of the state's motor-vehicle code").

[58] *See* Martin v. Herzog, 126 N.E. 814, 815 (N.Y. 1920) (discussing negligence predicated on failure to stay to the right of the center of the highway, as required by statute).

[59] *See id.* at 815 (holding that the failure of a wagon driver to display the lights required by a highway law was negligence).

[60] *See* Griffith v. Schmidt, 715 P.2d 905, 911 (Idaho 1985) (holding that exceeding the speed limit was negligence *per se*).

[61] RESTATEMENT, THIRD, OF TORTS: LIABILITY FOR PHYSICAL HARM § 14 cmt. e (Proposed Final Draft No. 1, 2005).

be done in given circumstances.

However, factors other than class of persons and type of harm may be taken into account in determining whether a statute that is silent as to civil liability appropriately defines what is expected of a reasonably prudent person. For example, a court should not embrace as the basis for civil liability a statute that is obsolete,[62] vague,[63] or duplicative of existing common-law obligations.[64] Similarly, if the legislature intended the penalties for violation of a law to be minimal or limited to those set forth in the enactment, a court should not rely on the law as a basis for imposing other legal obligations.[65]

The GLBA is an important expression of public policy that courts should take into account in determining whether database possessors, or some subset thereof (e.g., financial institutions or businesses generally), have a legal duty enforceable in a tort action to protect information relating to data subjects.[66] Indeed, as an enactment of Congress, the nation's highest legislative body, the language of the GLBA is entitled to great weight in resolution of the duty question. However, the GLBA itself should not be interpreted as setting the standard of care for a civil cause of action because it lacks specificity as to precisely what is required of a reasonable financial institution.[67] In contrast to a law that gives clear notice of what is expected–such as a statute that requires a pedestrian to walk on the sidewalk, not in the street,[68] or to "yield the right

---

[62] RESTATEMENT, SECOND, OF TORTS § 286 cmt. d (1965) (discussing obsolescence).

[63] *See, e.g.*, Perry v. S.N., 973 S.W.2d 301 (Tex. 1998) (holding that a statute imposing a reporting requirement on any person having "cause to believe" that a child was being abused was not an appropriate standard for negligence *per se* liability because, among other things, the statutory standard was not clearly defined).

[64] *See generally* RESTATEMENT, THIRD, OF TORTS: LIABILITY FOR PHYSICAL HARM § 14 cmt. e (Proposed Final Draft No. 1, 2005) (discussing statutes duplicating the common law).

[65] *See id.* at § 14 cmt. c (stating that if a statute includes a provision making the statute irrelevant in a common-law action for damages, courts should honor it). *See also* Pool v. Ford Motor Co., 715 S.W.2d 629 (Tex. 1986) (holding that the lower court erred in relying on two statutes, one of which provided that the presumption of intoxication would not apply in civil actions, and another which stated that "maximum or minimum speed limitations shall not be construed to relieve the plaintiff in any action from the burden of proving negligence").

[66] *See* CRITICAL INFORMATION INFRASTRUCTURE, *supra* note 12, at 46 n.29 that "[i]t could be argued that financial institutions have an existing duty under the Gramm-Leach-Bliley implementing regulations to provide immediate and effective incident response to protect the confidentiality of consumer data maintained on their own networks").

[67] *Cf.* County of Dallas v. Poston, 104 S.W.3d 719 (Tex. App. 2003) (holding that, because the statutory duty of a motor vehicle operator crossing a highway to yield the right-of-way to an approaching vehicle is not absolute, the statute was not a proper basis for a finding of contributory negligence as a matter of law; the appropriate inquiry is whether a reasonably prudent driver under the same or similar circumstances would have yielded the right-of-way).

[68] *See* Zeni v. Anderson, 243 N.W.2d 270, 273 (Mich. 1976) (discussing a sidewalk statute).

of way to all vehicles upon the roadway"[69]–the GLBA offers no clear guidance as to exactly what a financial institution must do to avoid liability. The act is vague. It speaks of an obligation to protect data security without indicating what must be done to fulfil that obligation. The vagueness of the GLBA, coupled with its failure to provide for civil liability, means that the questions of whether there is a tort duty, and if so what that duty requires, are still issues that must be resolved by the courts. Of course, "the presence of a statutory requirement that is binding on the defendant, and the court's awareness of the legislature's assumptions in imposing that requirement, can be important points for the court to consider in determining whether a duty exists."[70] But the question of duty requires judicial determination. Consequently, insofar as the GLBA is concerned, it is not useful to speak of negligence *per se*.[71]

The same analysis would not necessarily apply to the regulations adopted pursuant to the mandates of the GLBA. Unlike the statute itself, the provisions adopted to implement its mandates might be sufficiently specific to define what action is required of financial institutions with regard to protecting data security. However, the standards that have been adopted, such as those issued by the Federal Trade Commission,[72] are typically flexible in nature, equivocal as to

---

[69] Ranard v. O'Neil, 531 P.2d 1000, 1003 (Mont. 1975).

[70] RESTATEMENT, THIRD, OF TORTS: LIABILITY FOR PHYSICAL HARM § 14 cmt. i (Proposed Final Draft No. 1, 2005).

[71] *Cf.* RESTATEMENT, THIRD, OF TORTS: LIABILITY FOR PHYSICAL HARM § 14 cmt. e (Proposed Final Draft No. 1, 2005):

> Many statutes impose obligations on actors that largely correspond to or codify obligations imposed by negligence law . . . . Thus a statute might require motorists to drive their vehicles at a "reasonable and prudent" speed, or might prohibit driving the vehicle "carelessly." To find that an actor has violated such a statute, the jury would also need to find that the actor has behaved negligently. In such situations, the doctrine of negligence *per se* is largely superfluous in ascertaining the actor's liability. . . . [C]ourts sometimes allow parties to argue negligence per se as a supplement to ordinary negligence; but more frequently they reject negligence *per se*, recognizing its redundancy. . . .

See also Louisiana-Pacific Corp. v. Knighten, 976 S.W.2d 674 (Tex. 1998) (holding that a statute governing the duty of a driver following another vehicle, which required the driver to proceed safely and safely bring a vehicle to a stop, imposed on the driver a duty of reasonable care, and precluded the leading driver from obtaining a negligence *per se* instruction in an action arising out of a rear-end collision).

[72] *See* Standards for Safeguarding Customer Information, 16 C.F.R. § 314.1 et seq. (Westlaw current through July 1, 2005). *See also* CRITICAL INFORMATION INFRASTRUCTURE, *supra* note 12, at 57-58 (stating that "On May 17, 2002, the FTC issued the Safeguards Rule, which implements the safeguard provisions required by the Gramm-Leach-Bliley Act. The Safeguards Rule requires covered entities to implement a comprehensive information security program by May 23, 2003, to ensure the security, confidentiality, and integrity of nonpublic customer information against both internal and external threats. Institutions that fail to comply could face potential FTC enforcement actions and potential liability under state consumer protection laws or common law claims (such as negligence)").

what must be done, and generally unsuited to defining the conduct expected of a reasonably prudent financial institution. The FTC standards require financial institutions subject to the commission's jurisdiction to develop and implement a written security plan "appropriate"[73] to their size and complexity, which takes into account various sources of risk,[74] regularly tests the effectiveness of its "safeguards' key controls, systems, and procedures,"[75] and is periodically adjusted as necessary.[76] Thus, the standards simply endorse a process by which financial institutions are required to address security issues. Like the GLBA itself, the FTC standards offer no clear guidance as to precisely what precautions must be implemented to protect data security. The same is true of the federal Interagency Guidelines Establishing Standards for Safeguarding Customer Information, which address the obligations imposed by the GLBA.[77] As yet, no reported cases have held that the data security provisions[78] of the GLBA, related regulations, or other federal laws[79] set the standard of care for a tort action by a customer against

---

[73] *See* 16 C.F.R. § 314.3(a) (stating that financial institutions "shall develop, implement, and maintain a comprehensive information security program that is written . . . and contains administrative, technical, and physical safeguards that are appropriate to your size and complexity, the nature and scope of your activities, and the sensitivity of any customer information at issue").

[74] *See* 16 C.F.R. § 314.4(b) (stating that "[a]t a minimum, . . . a risk assessment should include consideration of risks in each relevant area of your operations, including: (1) Employee training and management; (2) Information systems, including network and software design, as well as information processing, storage, transmission and disposal; and (3) Detecting, preventing and responding to attacks, intrusions, or other systems failures").

[75] 16 C.F.R. § 314.4(c).

[76] *See* 16 C.F.R. § 314.4(e) (requiring adjustments in light of "any material changes to your operations or business arrangements; or any other circumstances that you know or have reason to know may have a material impact on your information security program").

[77] *See* 12 CFR Pt. 30, App. B (Westlaw current through July 1, 2005). One provision in the Interagency Guidelines that has some degree of specificity concerns service providers. The Guidelines state that "[e]ach bank shall . . . [r]equire its service providers by contract to implement appropriate measures designed to meet the objectives of these Guidelines." *Id*. However, it is doubtful whether this rule would be a helpful standard for resolving tort litigation by customers. The plaintiff would have to show that not only did the service provider not employ appropriate safeguards, but that except for the absence of a contractual provision that would not have occurred. Such a finding would entail a degree of speculation by the fact finder, and might present the type of causation problem that is sufficient to dissuade a court from embracing a rule as establishing the threshold for liability. *See* Stachniewicz v. Mar-Cam Corp., 488 P.2d 436 (Or. 1971) (declining to hold that a dram shop statute set the standard of care because it would complicate the causation assessment).

[78] The GLBA also extensively regulates the sharing of personal data between institutions. A violation of those provisions does not give an affected individual a private cause of action. *See* Menton v. Experian Corp., 2003 W.L. 21692820, *3 (S.D.N.Y.) (finding. in dicta, no private right of action).

[79] *See generally* Preston & Turner, *supra* note page 7, at 471-77 (discussing data security provisions in the Health Insurance Portability & Accountability Act of 1996 (HIPAA) and

a financial institution.

2. State Security Breach Notification Laws

Certain state security breach notification laws that require database possessors to protect personal information from unauthorized access make no provision for civil liability.[80] Some of these laws may nevertheless leave room for judicial recognition of a civil cause of action. For example, the Arkansas Personal Information Protection Act,[81] which provides only for enforcement by the attorney general,[82] states that the act "does not relieve a person or business from a duty to comply with any *other* requirements of *other* state and federal law regarding the protection and privacy of personal information."[83] However, the use of the word "other" seems to suggest that the security breach notification law should not, by itself, be embraced by a court as the basis for a civil cause of action.

Similarly, it is difficult to envision that the Texas state security breach statute could be used as a predicate for a negligence *per se* claim. The Texas law,[84] like its California predecessor, [85] obliges a database possessor to exercise care to protect the personal information of data subjects.[86] However, unlike the California SBIA,[87] the Texas act does not create a civil cause of action against a database possessor who fails to exercise reasonable care. Indeed, while the Texas act is silent on that subject, it expressly provides for a deceptive trade practices

---

Children's Online Privacy Protection Act (COPPA)).

[80] *See* R.I. GEN. LAWS. § 11-49.2-2(2) *et seq.*, R.I. Legis. 05-225 (providing that "A business that owns or licenses computerized unencripted personal information about a Rhode Island resident shall 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"). Each violation of the Rhode Island law "is a civil violation for which a penalty of not more than a hundred dollars ($100) per occurrence and not more than twenty-five thousand dollars ($25,000) may be adjudged against a defendant"). *Id.* at § 11-49.2-6(a).

[81] ARK. CODE ANN. § 4-110-104(b), Ar. Legis. 1526 (2005) (requiring a "person or business that acquires, owns, or licenses personal information about an Arkansas resident . . . [to] 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").

[82] *Id.* at § 4-110-108.

[83] Id. at § 4-110-106(b) (italics added).

[84] TEX. BUS. & COM. CODE § 48.001 *et seq.*, Tx. Legis. 294 (2005).

[85] CAL. CIV. CODE § 1798.81.5(b) (Westlaw current through Ch. 33 of 2005 Reg. Sess. urgency legis. & Gov. Reorg. Plan No. 2 of 2005).

[86] TEX. BUS. & COM. CODE § 48.102(a) (providing that "[a] business shall implement and maintain reasonable procedures, including taking appropriate corrective action, to protect and safeguard from unlawful use or disclosure any sensitive personal information collected or maintained by the business . . .").

[87] *See* CAL. CIV. CODE § 1798.84.

action[88] against hackers and others who obtain, possess, transfer, or use the personal information of another without authorization.[89] It would be reasonable to interpret the Texas statute as an expression that civil liability should extend thus far (to hackers and other unauthorized persons) and no further (to database possessors). *Expressio unius est exclusio alterius*.[90] That construction of the law could be supported on public policy grounds, namely that judicial deference to a co-equal branch of government[91] means that a court should not create a cause of action where the legislature has implicitly determined that none should exist.[92]

C. Basic Tort Principles

1. *Palsgraf*, *Kline*, and Related Cases

Turning to the issue of whether common-law principles–as opposed to statutes–support judicial recognition of a duty on the part of database possessors to safeguard information from intruders, it is useful to consider the guidance offered by two landmark cases: *Palsgraf v. Long Island Railroad Co.*[93] and *Kline v. 1500 Massachusetts Avenue Apartment Corporation*.[94] Each of these decisions has appeared in countless tort casebooks and has been cited scores of times by judicial decisions. *Palsgraf* and *Kline* are important pillars in the temple of American tort law.

In *Palsgraf*, the most famous tort case of all time, the majority opinion was written by Chief Judge Benjamin Cardozo, the "most justly celebrated of American common-law judges."[95]

---

[88] TEX. BUS. & COM. CODE § 48.203.

[89] *See* TEX. BUS. & COM. CODE § 48.101 (providing that "[a] person may not obtain, possess, transfer, or use personal identifying information of another person without the other person's consent and with intent to obtain a good, a service, insurance, an extension of credit, or any other thing of value in the other person's name").

[90] To "express or include one thing implies the exclusion of the other, or of the alternative." BLACK'S LAW DICTIONARY (8th ed. 2004).

[91] *See* JOHNSON & GUNN, *supra* note 33, at 9 (noting that it is a policy foundation of American tort law that "[c]ourts should accord due deference to co-equal branches of government"; "there are occasions when the judiciary should eschew action in favor of other branches. . . . [C]ertain questions are best left to the legislature because of its ability to gather facts through the legislative hearing process, to craft comprehensive solutions to broad-ranging questions, or to represent the will of the public on highly controversial issues").

[92] *Cf.* Bruegger v. Faribault County Sheriff's Dept., 497 N.W.2d 260 (Minn. 1993) (holding that a violation of the Crime Victims Reparations Act (CVRA) did not create a private cause of action against law enforcement agencies which failed to inform the plaintiffs of their rights to seek reparations; "[p]rinciples of judicial restraint preclude us from creating a new statutory cause of action that does not exist at common law where the legislature has not either by the statute's express terms or by implication provided for civil tort liability").

[93] 162 N.E. 99 (N.Y. 1928).

[94] 439 F.2d 477 (D.C. Cir. 1970).

[95] JOHN T. NOONAN, JR., PERSONS AND MASKS OF THE LAW: CARDOZO, HOLMES, JEFFERSON, AND WYTHE AS MAKERS OF THE MASKS 111 (1976).

Cardozo set down the basic rule on duty for the New York Court of Appeals. "The risk reasonably to be perceived defines the duty to be obeyed and risk imports relation; it is risk to another or to others within the range of apprehension."[96] In *Palsgraf*, there was nothing in the appearance of a newspaper-wrapped package being carried by a man trying to board a moving train that gave notice that the parcel contained explosives. Therefore, there was nothing to warn the trainmen that, if the package was dropped, Helen Palsgraf, a patron waiting across the platform, was in danger. There was no "risk [to her] reasonably to be perceived," and thus no "duty [to her] to be obeyed." So far as she was concerned, the railroad was under no legal obligation not to carelessly dislodge the package while trying to assist the man who was running for the train, but "seemed unsteady as if about to fall."[97] Because there was no duty to Palsgraf, the railroad was not liable in negligence for the harm she sustained when the package fell and exploded.

Courts today continue to apply the *Palsgraf* duty rule.[98] Thus, it is useful to ask whether, from the standpoint of database possessors, there is a "risk reasonably to be perceived"[99] to data subjects if data is not protected from unauthorized intrusion. Obviously, in many situations (such as where data is accessible to hackers via the Internet), the answer is "yes." The risk is entirely foreseeable and a threat to the interests of data subjects is "within the range of apprehension."[100] At least on its face, the basic rule in *Palsgraf* suggests that database possessors should often have a duty to exercise reasonable care to protect data from intruders."

Palsgraf did not involve the threat of criminal intervention, but *Kline* did. In *Kline*, a landlord was on notice that an increasing number of assaults, larcenies, and robberies were being perpetrated on tenants in the common areas of a large apartment building. In holding the landlord responsible for a subsequent attack on the plaintiff, the court said that a landlord is by no means an insurer of the safety of its tenants and is not obliged to provide protection commonly afforded by a police department. However, a landlord is under a duty to take such precautions as are within its power and capacity to prevent harm by criminal intruders.[101] In writing for the D.C. Circuit, Judge Malcolm Richard Wilkey emphasized the fact that the landlord was the only party in a position to secure the common areas:

> No individual tenant had it within his power to take measures to guard the garage entranceways, to provide scrutiny at the main entrance of the building, to patrol the

---

[96] 162 N.E. at 100.

[97] 162 N.E. at 99.

[98] *See, e.g.*, Holder v. Mellon Mortgage Co., 5 S.W.3d 654 (Tex. 1999) (deciding, with reliance on *Palsgraf*, that the owner of a parking garage was not responsible for an attack on the third-person perpetrated there by a stranger in the middle of the night because there was no reason to foresee that the attacker or victim would be present at that hour).

[99] 162 N.E. at 100.

[100] *Id*. at 100.

[101] 439 F.2d at 488 (stating that a landlord's "duty is to take those measures of protection which are within his power and capacity to take, and which can reasonably be expected to mitigate the risk of intruders assaulting and robbing tenants").

> common hallways and elevators, to set up any kind of a security alarm system in the building, to provide additional locking devices on the main doors, to provide a system of announcement for authorized visitors only, to close the garage doors at appropriate hours, and to see that the entrance was manned at all times.[102]

The court added:

> The landlord is entirely justified in passing on the cost of increased protective measures to his tenants, but the rationale of compelling the landlord to do it in the first place is that he is the only one who is in a position to take the necessary protective measures for overall protection of the premises . . . .[103]

A similar analysis is equally applicable to cases involving database security. Individual data subjects are in a poor position to do anything to protect database information about them from intruders.[104] The database possessor, in contrast, is the only one with the ability to mitigate the risk that intruders may cause harm. As in *Kline*, the cost of providing database security could be spread to a broader class of data subjects, at least in cases where there is a customer relationship between the plaintiff and defendant. *Kline*, like *Palsgraf*, suggests that, at least in some circumstances, database possessors should owe data subjects a duty to exercise reasonable care to protect data from intruders.

In both *Palsgraf* and *Kline*, there was a relationship between the plaintiff and the defendant. Palsgraf was a ticket purchaser of the defendant railroad; Kline was a tenant of the defendant corporation. Those relational ties are important, for other cases teach that duty often depends upon more than foreseeability of harm and opportunity to take precautions–it depends, sometimes, on a special linkage between the party on whom the duty would be imposed and the one who would be benefited. In this regard, the recent cases involving allegedly negligent enablement of imposter fraud[105] are instructive.

In *Huggins v. Citibank, N.A.*,[106] for example, the plaintiff sued various banks on the ground that they negligently issued credit cards in the plaintiff's name to an unknown imposter. The plaintiff alleged, among other things, that the banks issued "credit cards without any

---

[102] *Id.* at 480.

[103] *Id.* at 488.

[104] *Cf.* White, *supra* note 3, at 852-53 (stating that "[f]requently, an individual does not know how much information is stored in his digital dossier, or who has compiled it. This makes it difficult, if not impossible, for an individual to control access to his personal information and, thus, limit his vulnerability to instances of identity theft").

[105] *See generally* Brendan Delaney, Comment, *Identity Theft: The Fair Credit Reporting Act and Negligent Enablement of Imposter Fraud*, 54 CATH. U. L. REV. 553, 556 (2005) (arguing for "greater federal protection for potential victims of identity theft and for common law judicial recognition of the tort of negligent enablement of impostor fraud").

[106] 585 S.E.2d 275 (S.C. 2003).

investigation, verification, or corroboration" of the applicant's identity.[107] In response, the banks asserted they owed no duty to the plaintiff because he was not their customer.[108] The court agreed with the defendants and wrote:

> In order for negligence liability to attach, the parties must have a relationship recognized by law as the foundation of a duty of care. . . . In the absence of a duty to prevent an injury, foreseeability of that injury is an insufficient basis on which to rest liability. . . .
>
> . . . .
>
> The relationship, if any, between credit card issuers and potential victims of identity theft is far too attenuated to rise to the level of a duty between them. . . .[109]

Other courts have reached similar conclusions.[110]

Together, *Palsgraf*, *Kline*, and *Huggins* indicate that the strongest cases for imposing a common-law duty to guard data from intruders will be those where there is a business relationship[111] between defendant database possessor and the plaintiff data subject. This makes sense on economic, as well as doctrinal, grounds. Imposing a duty of care in such cases will force the database possessor, who benefits from the use of computerized information, to internalize losses relating to improperly accessed data as a cost of doing business.[112] That, in

---

[107] 585 S.E.2d at 276.

[108] 585 S.E.2d at 276.

[109] 585 S.E.2d at 277.

[110] *See, e.g.*, Smith v. Citibank, 2001 WL 34079057 (W.D. Mo. 2001) (holding that a credit card issuer is not liable in negligence to a non-customer); Polzer v. TRW, Inc., 682 N.Y.S.2d 194 (App. Div. 1998) (similar).

[111] Sometimes a business relationship is proposed but not consummated, such as where an applicant applies to a university, but is not accepted for admission. The business (university) benefits from solicitation and review of applications, so it may be fair to impose on the institution an obligation to safeguard the data of the applicant so long as that data is retained. The same would seem to be true where the relationship has effectively ended, as in the case where a student has graduated. *Cf.* Stacy Finz, Hackers Hit College Computer System, San Fran. Chron., Aug. 9, 2005 (discussing hackers who gained access to the records of 61,709 persons "who either attended, applied, graduated or worked" at Sonoma State University).

[112] *See* JOHNSON & GUNN, *supra* note 33, at 7-8 (stating that "[i]t has often been urged that . . . [t]hose who benefit from dangerous activities should bear resulting losses. Certain activities–*e.g.*, owning a dog that may bite or using explosives–entail a serious risk of harm to third persons even if care is exercised by the actor. According to this principle, fairness requires that those who enjoy the benefits of such conduct should bear resulting losses . . . . In a related vein, it is sometimes said that an activity 'must pay its own way.' What this means is that there is good reason for the law to force the promoters of activities to 'internalize' the costs that their endeavors inflict on third persons. Only when those costs are taken into account, it is argued, are promoters likely to make decisions that are not only personally beneficial, but socially

turn, will create an incentive for database possessors to scrutinize whether their business methods are really worth the costs they entail. At the same time, the imposition of a duty in a business context gives the database possessor a means for distributing the loss through price adjustments of goods or services sold to the class of persons which ultimately benefits from the defendant's business methods. That reallocation of losses will help to ensure that the costs relating to improperly accessed data will not fall with crushing weight on either the data subject or the database possessor.[113]

2. Public Policy Analysis

In addressing questions of duty in areas of the law that are not well settled,[114] courts often ask whether imposition of duty makes sense as a matter of public policy. They consider, for example, whether obligating the defendant to exercise care would tend to minimize harm to potential plaintiffs without being unduly burdensome to the defendant or disruptive to the community.[115] Courts also sometimes consider "the availability, cost, and prevalence of insurance for the risk involved,"[116] with the assumption being that insurability of the risk makes imposition of a duty more palatable because the costs of the harm can be spread broadly. On each of these grounds–deterrence of losses, burden to the defendant, community consequences, and insurance–a good argument can be made for requiring database possessors to exercise care to prevent harm by intruders.

Placing a burden on database possessors to protect data from unauthorized access would tend to reduce intruder-related losses by encouraging investment in database security.[117] That investment would be consistent with the possessors' own interests because unauthorized access entails huge costs for those who maintain databases.[118] Companies must spend large sums of

---

responsible").

[113] *But see* JOHNSON & GUNN, *supra* note 33, at 743 (discussing the limits of risk spreading).

[114] *Cf.* Rustad, *supra* note 2, 6, at 108 (stating that "[i]t is unclear . . . whether a website owes a general duty of care to website visitors when there is no statutorily mandated standard of care").

[115] *See* Rowland v. Christian, 70 Cal. Rptr. 97, 100 (Cal. 1968) (indicating that among the policy considerations typically deemed relevant to whether a duty to act should be imposed are "the moral blame attached to the defendant's conduct, the policy of preventing future harm, the extent of the burden to the defendant and consequences to the community of imposing a duty to exercise care with resulting liability for breach").

[116] Rowland v. Christian, 70 Cal. Rptr. 97, 100 (Cal. 1968).

[117] *See* CRITICAL INFORMATION INFRASTRUCTURE, *supra* note 12, at 45 (opining that "[i]f tort law is found to apply to computer security, then the potential for civil liability lawsuits (with the likelihood of monetary damages) could encourage companies to invest in computer security measures").

[118] *See* Wibel, *supra* note 12, at 1578 (stating that "[e]ven a nonmalicious trespass disrupts the victim's online services while the breach is fixed. . . . [C]ompanies generally expend resources investigating the matter, often hiring private investigators so that they do not

money to protect their websites[119] and other data sources, as well as to cover resulting harm when protection efforts are unsuccessful.[120] "The financial losses facing corporate America as a result of network security breaches are staggering–hundreds of millions, if not billions, of dollars each year . . . ."[121] The burden entailed by the imposition of a legal duty would by no means be solely for the benefit of potential plaintiffs.

The imposition of a common-law tort duty to protect databases would also be consistent with the developing fabric of the law. As the preceding discussion suggests, an increasing number of statutes[122] and regulations,[123] as well as commentators,[124] say that reasonable care must be exercised to protect computerized personal data from unauthorized access. Thus, recognition of a tort duty to protect data would not be disruptive to the community. It would not require new institutions or controversial practices. Indeed, a common-law tort duty to protect data would be complementary of recent developments in both the law and business.

The liability risks arising from data intrusion can be spread[125] by insurance, and policies are now being offered.[126] Of equal importance, insurers can and do provide guidance to their

---

suffer reputational loss").

[119] *See* Rustad, *supra* note 2, 6, at (stating that in 2000, "private companies spent an estimated $300 billion in private enforcement efforts against hackers and viruses").

[120] *See* Wibel, *supra* note 12, at 1597-98 (reporting that "[c]omputer crime cost about $250 million in 1998 and jumped to more than $375 million in 2001. . . . In 2000, private companies spent an estimated $300 billion in private enforcement efforts against hackers and viruses").

[121] *See* Steinberg, *supra* note 22, at 60.

[122] Presumably, judicial willingness to recognize a common-law duty to protect databases is increased by the existence of state security breach notification laws. *Cf.* Paetkau & Torabian-Bashardoust, *supra* note 39, at 39 (discussing the California law's obligation to disclose security breaches and opining that "from a legal perspective, if the company notifies only California residents of a security breach, potentially affected non-Californian residents could persuasively argue that the company was at least negligent in not notifying them of the breach").

[123] *See* Part II-B-1 (discussing the regulations adopted pursuant to the GLBA).

[124] *See* Erin E. Kenneally, *Stepping on the Digital Scale: Duty and Liability for Negligent Internet Security*, 1 Ann. 2002 ATLA-CLE 403 (2002) (discussing the liability of companies doing business on the web).

[125] *See* JOHNSON & GUNN, supra note 33, at 7 (noting that in the development of American tort law it has often been urged that "[t]he costs of accidents should be spread broadly. The idea underlying the 'spreading' rationale is that the financial burden of accidents may be diminished by spreading losses broadly so that no person is forced to bear a large share of the damages. . . . Losses can be spread not only through increases in the costs of goods and services, but through other devices such as taxation and insurance").

[126] *See* Steinberg, *supra* note 22, at 60 (stating that "[s]tand-alone network-risk, hacker, or cyber insurance is now being offered . . . . [T]hese policies offer protection against intangible data loss from viruses, denial-of-service attacks, and theft of consumer information–and the

insureds about practices calculated to minimize liability.[127] That advice helps to reduce the frequency and amount of future losses, and thereby reinforces the deterrence objectives of the law.

Imposing a tort duty under which database possessors will be held liable for negligent data security practices will inevitably leave many questions unanswered. To say that an enterprise has a duty to exercise reasonable care to ensure data security provides no clear guidance as to very practical questions, such as how often patches should be applied to security software.[128] But these types of questions are no different than those faced in a thousand other settings where courts apply the rules of negligence liability. Over the long run, the burden of uncertainty is minimized by evolving guidance found in scholarship discussing court decisions and legislation,[129] as well as by the development of industry customs[130] and the promulgation of regulations which help to define what conduct is required of a potential defendant seeking to avoid liability.

3. Voluntary Assumption of Duty

Even if courts decline to impose a tort duty to safeguard data on database possessors generally (or at least on businesses), a legally enforceable data-protection obligation may be

---

protection can extend to third-party liabilities. Insurance premiums remain considerable, and prequalifying security assessments can be demanding; moreover, legal advice is often a pre-requisite for navigating the various gaps and exclusions written into such policies").

[127] *See* Jay P. Kesan, Ruperto P. Majuca, & William J. Yurcik, *The Economic Case for Cyberinsurance*, in SECURING PRIVACY IN THE INTERNET AGE __ (Stanford Univ. Press 2005), *available at* http://ssrn.com/abstract=577862 (last visited Aug. 10, 2005) (stating that "cyberinsurance facilitates standards for best practices as cyberinsurers seek benchmark security levels for risk-management decisionmaking"); CRITICAL INFORMATION INFRASTRUCTURE, *supra* note 12, at 65-66 (discussing how the insurance industry can motivate responsible practices in the private sector).

[128] *See* CRITICAL INFORMATION INFRASTRUCTURE, *supra* note 12, at 51 (discussing the problem).

[129] *See* Thomas J. Smedinghoff, *The Developing U.S. Legal Standard for Cybersecurity* The Sedona Conference Journal, June, 2003, *available at* http://www.bakernet.com/ecommerce/us cybersecurity standards.pdf) (last visited Aug. 9, 2005) (discussing "laws and regulations requiring security" and "the developing trend as to what businesses must do to satisfy their legal obligations to provide appropriate security").

[130] *See* CRITICAL INFORMATION INFRASTRUCTURE, *supra* note 12, at 50 (stating that "[a]s a motivating factor for industry to adopt best practices, tort law can be a significant complement to standard-setting, because compliance with industry-wide standards is usually an acceptable demonstration of due care"); Randy V. Sabett, *Graceful Disclosure: The Pros & Cons of Mandatory Reporting of Security Vulnerabilities*, 4 SEDONA CONF. J. 121, 124 (2003) (stating that "several organizations have developed vulnerability disclosure policies" relating to software).

recognized under voluntary-assumption-of-duty principles.[131] A person who is not otherwise under a duty to exercise reasonable care may voluntarily assume the responsibility to do so. One way of doing that is by promising to exercise care and thereby inducing detrimental reliance.[132] Another way is by entering upon an "undertaking" and consequently increasing the risk of harm to the plaintiff.[133] Either way, if the voluntarily assumed duty is breached and causes damage, the party who undertook the duty of reasonable care will be subject to liability.

These well-established principles might be found to apply to situations where consumers reveal personal information to financial institutions in reliance upon their stated privacy policies.[134] For example, the policy of one major banking institution, which is not atypical, states in reassuring terms:

> The law gives you certain privacy rights. Bank of America gives you more. . . .
>
> . . . .
>
> Keeping financial information secure is one of our most important responsibilities. We maintain physical, electronic and procedural safeguards to protect Customer Information.
>
> . . . .
>
> . . . . All companies that act on our behalf are contractually obligated to keep the information we provide to them confidential . . . .[135]

A customer reading this information would conclude, at a minimum, that in exchange for being entrusted with personal information, the bank had agreed (1) to protect the data by means of physical, electronic, and procedural safeguards and (2) keep it confidential. Those very sensible conclusions would be reinforced by other language in the privacy policy stressing the importance of precautions on the part of the customer to guard against disclosure or

---

[131] *See generally* RESTATEMENT, THIRD, OF TORTS: LIABILITY FOR PHYSICAL HARM § 42 (Proposed Final Draft No. 1 2005) (discussing duty based on undertaking).

[132] *See id.* at § 42 cmt. e (discussing promises as undertakings).

[133] *See id.* at § 42(a) (providing that "[a]n actor who undertakes to render services to another that the actor knows or should know reduce the risk of physical harm to the other has a duty of reasonable care to the other in conducting the undertaking . . . if the failure to exercise such care increases the risk of harm beyond that which existed without the undertaking").

[134] *See generally* Therese G. Franzén & Leslie Howell, *Financial Privacy Rules: A Step By Step Guide to the New Disclosure Requirements Under the Gramm-Leach-Bliley Act and the Implementing Regulations*, 55 CONSUMER FIN. L.Q. REP. 17, 20-21 (2001) (discussing privacy notices).

[135] Bank of America Privacy Policy for Customers 2005, at http://www.bankofamerica.com/privacy/index.cfm?template=privacysecur_cnsmr .

unauthorized use of account and personal information.[136] The same is true of statements in the bank's advertising[137] or on its website emphasizing the dangers of identity theft and assuring the customer that "[y]our statements are always protected in Online Banking. . . ."[138] A court might reasonably interpret such a privacy policy as an undertaking to exercise reasonable care, and might conclude that a breach of that duty would support a tort cause of action.

Similarly, even if the plaintiff never read or relied on the institution's privacy policy, a duty of care might be imposed under the other prong of the undertaking rule which says that, where services provided for the protection of another increase the risk of harm beyond that which existed without the undertaking, there is a duty to exercise reasonable care.[139] Depending on the facts, the measures (e.g., use of passwords, firewalls, etc.) taken to protect computerized data may contain flaws which increase the risk of unauthorized data access. An increased risk of harm might also result where data protection practices allow transmission of unencrypted data, which is especially vulnerable to hacking. To these types of cases, the increased-risk rule might apply.

According to the Restatement provision on undertakings, negligence liability that is based on inducing detrimental reliance or increasing the risk of injury is limited to compensation for physical harm. This is a significant limitation which presumably means that the economic losses associated with identity theft are not recoverable under this theory of duty. However, a database possessor might still be liable under the undertaking rule for personal injury or property damage perpetrated on a data subject by an intruder or one who obtained personal information from that person.

D. Fiduciary Obligations

A fiduciary is one who voluntarily[140] holds a position of special trust and confidence which obliges the fiduciary to act in the best interest of another.[141] The duties imposed on a

---

[136] *Id.* (discussing the topic in detail).

[137] *See* Dash, *supra* note 10 (reporting that "financial services and technology companies have been quietly tweaking their advertising to incorporate themes about the safety of customers' data").

[138] Bank of America website, at http://onlineeast1.bankofamerica.com/cgi-bin/ias/flYwcybDuvu4kiYniTVL45Ia4908NK+4u_DQKNhH37344/2/bofa/ibd/IAS/presentation/WelcomeControl?action=protect_my_account_string .

[139] *See* RESTATEMENT, THIRD, OF TORTS: LIABILITY FOR PHYSICAL HARM § 42(a) (Proposed Final Draft No. 1 2005) (discussing increased risk of harm).

[140] *See* PulseCard, Inc. v. Discover Card Services, Inc., 917 F. Supp. 1478, 1484 (D. Kan.1996) (stating that "[t]he hallmark of a fiduciary relationship is a voluntary and conscious assumption or acceptance of the duties of a fiduciary").

[141] *See* RESTATEMENT, SECOND, OF TORTS § 874 cmt. a (1979) (stating that "[a] fiduciary relation exists between two persons when one of them is under a duty to act for or to give advice for the benefit of another upon matters within the scope of the relation").

fiduciary–including loyalty, candor, and confidentiality–are sometimes co-extensive with those embraced by the law of negligence.[142] However, depending on the circumstances, fiduciary obligations may extend considerably further than a duty of reasonable care.[143]

If a database possessor owes fiduciary obligations to a data subject, it may reasonably be argued that regardless of whether general tort principles would impose such a duty, the fiduciary is obliged to protect computerized information relating to the data subject from unauthorized access by third parties.[144] For example, the relationship between an attorney and client is fiduciary as a matter of law.[145] Accordingly, lawyers have a special fiduciary obligation to protect confidential client information, aside from any demands imposed by ordinary tort principles. A lawyer's broad fiduciary obligation of confidentiality extends to all forms of information about the client.[146] This includes computerized data,[147] as well as information

---

[142] *See* Vincent R. Johnson & Shawn M. Lovorn, *Misrepresentations by Lawyers about Credentials or Experience*, 57 OKLA. L. REV. 529, 544 (2004) (noting that while "[s]ome courts have said that attorneys owe clients a duty of 'absolute and perfect candor' . . . [that] is an overstatement of an attorney's disclosure obligations, for in many contexts the law imposes no more than a duty of reasonable care to keep a client informed of relevant matters").

[143] *See* Vincent R. Johnson, *"Absolute and Perfect Candor" to Clients*, 34 ST. MARY'S L.J. 737, 792 (2003) (indicating that if the interests of lawyer and client diverge, the lawyer's duty is essentially one of absolute and perfect candor).

[144] Fiduciary-duty principles are drawn from many areas of the law, including the rules governing trusts, corporations, and agency. At least in some contexts, a breach of fiduciary duty is treated as a type of tort. *See* RESTATEMENT, SECOND, OF TORTS § 874 (1979) (stating that "[o]ne standing in a fiduciary relation with another is subject to liability to the other for harm resulting from a breach of duty imposed by the relation").

[145] *See, e.g., Keywell Corp. v. Piper & Marbury, L.L.P.*, 1999 W.L. 66700, at *4 (stating that "it is axiomatic that the relationship between an attorney and his or her client is a fiduciary one").

[146] *See* RESTATEMENT, THIRD, OF THE LAW GOVERNING LAWYERS § 59 (2000) (providing that "[c]onfidential client information consists of information relating to representation of a client, other than information that is generally known").

[147] *See* N.Y. State Bar Assn. Comm. on Prof'l Ethics, Opinion No. 782 (2004) (stating that "[w]hen a lawyer sends a document by e-mail, as with any other type of communication, a lawyer must exercise reasonable care to ensure that he or she does not inadvertently disclose his or her client's confidential information. . . . Reasonable care may, in some circumstances, call for the lawyer to stay abreast of technological advances and the potential risks in transmission in order to make an appropriate decision with respect to the mode of transmission"). *See generally* Jonathan Bick, *Client Internet Services Expose Firms to New Liability*, N.J. L.J., Sept. 20, 2004, available at http://www.bicklaw.com/Publications/Client_internet_to_Liability.htm (last visited Aug. 9, 2005) (indicating that client services now include "offering clients protected access to their personal case information over the Internet" and stating that "ethical rules . . . [are] equally applicable to Internet transactions"); David Hricik, *The Speed of Normal: Conflicts, Competency, and Confidentiality in the Digital Age*, 9 COMPUTER L. REV. & TECH. J. ____, ____ (2005) (discussing ethical obligations of attorneys relating to digitally stored client confidences).

contained in printed documents or otherwise known by the attorney,[148] for the existence of the duty turns on the content, not the form, of the information.[149] In light of the fiduciary-duty rules on confidentiality (and the related obligations requiring safekeeping of client property[150]), a lawyer or law firm could not plausibly argue that there is no duty to safeguard computerized client data from intruders.

The same analysis should apply to all fiduciary relationships,[151] including those which are fiduciary as a matter of law (such as trustee-beneficiary[152]) and others which are fiduciary as a matter of fact because they entail a high degree of trust and confidence.[153] Importantly, however, ordinary business relationships are not fiduciary.[154] In business, parties normally deal with one

---

[148] *See* N.Y. Eth. Op. 643 (Feb. 16, 1993) (stating that client "files should be stored in a secure location").

[149] *See* RESTATEMENT, THIRD, OF THE LAW GOVERNING LAWYERS § 60 cmt. d (2000) (stating that "a lawyer who acquires confidential client information has a duty to take reasonable steps to secure the information against misuse or inappropriate disclosure . . . . This requires that client confidential information be acquired, stored, retrieved, and transmitted under systems and controls that are reasonably designed and managed to maintain confidentiality"). *See also* ABA Formal Op. 95-398 (stating that "[a] lawyer who gives a computer maintenance company access to information in client files must make reasonable efforts to ensure that the company has in place, or will establish, reasonable procedures to protect the confidentiality of client information"). *Cf.* ABA Formal Op. 99-413 (stating that "[l]awyers have a reasonable expectation of privacy in communications made by all forms of e-mail, including unencrypted e-mail sent on the Internet, despite some risk of interception and disclosure . . . [and] therefore . . . its use is consistent with the duty . . . to use reasonable means to maintain the confidentiality of information relating to a client's representation).

[150] *See* RESTATEMENT, THIRD, OF THE LAW GOVERNING LAWYERS § 44 (2000) (discussing the duty to safeguard and segregate client property).

[151] *Cf.* PulseCard, Inc. v. Discover Card Services, Inc., 917 F. Supp. 1478, 1484 (D. Kan. 1996) (stating that "almost every fiduciary relationship implies some duty of confidentiality").

[152] *See* PulseCard, Inc. v. Discover Card Services, Inc., 917 F. Supp. 1478, 1483 (D. Kan. 1996) (discussing fiduciary relationships "specifically created by contract such as principal/agent, attorney/client, and trustee cestui que trust"); RESTATEMENT, SECOND, OF TORTS § 874 cmt. b (1979) (referring to trustee, guardian, executor, and administrator).

[153] *See* Martinelli v. Bridgeport Roman Catholic Diocesan Corp., 196 F.3d 409, 429 (2d Cir. 1999) (finding that "irrespective of the duties of the Diocese to its parishioners generally, the jury could reasonably have found that the Diocese's relationship with [the plaintiff] was of a fiduciary nature"); Curl v. Key, 316 S.E.2d 272 (N.C. 1984) (holding that a confidential relationship existed and that the deed could be set aside on grounds of fraud where the defendant, who was referred to as "uncle" by the plaintiffs and who was the best friend of their deceased father, secured the plaintiffs' signatures on a "peace paper"); Navistar Intern. Transp. Corp. v. Crim Truck & Tractor Co., 791 S.W.2d 241, 242 (Tex. App.—Texarkana 1990) (indicating that informal relationships may be fiduciary).

[154] *See, e.g.*, PulseCard, Inc. v. Discover Card Services, Inc., 917 F. Supp. 1478, 1484 (D. Kan. 1996) (stating that "fiduciary obligations should be extended reluctantly to commercial

another at "arms length."[155] The "mere acceptance of confidential information" does not create a fiduciary relationship,[156] nor does the fact that one party "trusts another and relies on a promise to carry out a contract."[157] Fiduciary relationships are the exception, not the rule. Even the relationship between a teacher and a student[158] or a university and its alumni[159] is usually not fiduciary in nature. Consequently, while fiduciary-duty law may play an important role in whether professionals, such as lawyers, physicians, or trustees, have a duty to protect from intruders the information of clients, patients, and beneficiaries, it will not set the standard of care in most commercial settings.

III. The Duty to Reveal Evidence of Security Breaches

It is important to distinguish the duty to protect data from intrusion from the duty to disclose information that data security has been breached. A statute might impose both obligations (as does California's SBIA[160]), or it might impose one duty but not the other. For example, the Louisiana Database Security Breach Notification Law[161] contains no explicit obligation to protect data, but requires notification of data subjects upon discovery that security has been breached.[162] In addition, as discussed below, common-law rules may distinguish the obligation to disclose from the obligation to protect. For example, under certain rules, one whose conduct, "even though not tortious," has created a continuing risk of physical harm to the plaintiff has an obligation to exercise care to prevent the harm from occurring or minimize the adverse consequences.[163] This may mean that even if a database possessor was not under a duty enforceable in a private civil action to protect a data subject's personal information from unauthorized access, a duty may arise as a result of the intrusion and the possessor may have an

---

or business transactions" and holding that relationship between a credit card company and a provider of transaction processing services was not fiduciary).

[155] *See* Pellegrini v. Cliffwood-Blue Moon Joint Venture, Inc., 115 S.W.3d 577 (Tex. App. 2003) (characterizing the relationship between a geophysicist contractor and a joint venture as an arms-length transaction).

[156] PulseCard, Inc. v. Discover Card Services, Inc., 917 F. Supp. 1478, 1485 (D. Kan. 1996).

[157] *See* Navistar Intern. Transp. Corp. v. Crim Truck & Tractor Co., 791 S.W.2d 241, 243 (Tex. App.–Texarkana 1990).

[158] *See* Ho v. University of Tex. at Arlington, 984 S.W.2d 672 (Tex. Ct. App. 1998) (holding there is no fiduciary relationship between students and professors as a matter of law).

[159] *See also* Brzica v. Trustees of Dartmouth Coll., 791 A.2d 990 (N.H. 2002) (finding no fiduciary relationship between college trustees and alumni).

[160] *See* CAL. CIV. CODE § 1798.81.5(b) (Westlaw current through Ch. 33 of 2005 Reg. Sess. urgency legislation & Gov. Reorg. Plan No. 2 of 2005) (specifying duty to "implement and maintain reasonable security procedures and practices"); *id.* at § 1798.82 (imposing duty to disclose breach of security).

[161] LA. REV. STAT. § 51:3071 *et seq*., La. Legis. 499 (2005).

[162] *Id.* at § 3074(A) (detailing duty to disclose).

[163] RESTATEMENT, THIRD, OF TORTS: LIABILITY FOR PHYSICAL HARM § 39 (Proposed Final Draft 2005).

obligation to reveal that the security of the data has been breached.[164]

A duty to reveal that database security has been compromised may be placed on potential defendants in at least four ways. First, the duty may be imposed by statute, either as a result of the law's express terms or as a result of judicial reliance on the statute as the proper expression of the standard of care.[165] Second, a duty may arise from common-law principles governing negligence liability generally.[166] Third, a duty might be imposed under the law of misrepresentation, which creates a duty to update previously accurate statements (e.g., relating to data security) that are the basis for pending or continuing reliance by the recipient of the statements.[167] Finally, as noted above, failure-to-act rules may require the exercise of reasonable care to avoid or minimize damages, if a database possessor's conduct has created a continuing risk of physical risk harm.[168]

A. Statutory Duties

At least eighteen states[169] now have adopted database security breach information acts which require certain types of database possessors (typically businesses,[170] but sometimes governmental agencies[171] or other persons or entities,[172] such as non-profit organizations[173]) to

---

[164] *See* Part III-B-3, *infra*.

[165] *See* Part III-A, *infra*.

[166] *See* Part III-B-1, *infra*.

[167] *See* Part III-B-2, *infra*.

[168] *See* Part III-B-3, *infra*.

[169] *See* note 25, *supra*.

[170] *See, e.g.,* MONT. CODE ANN. § 31-3-115(5)(1)(a) and (7), Mt. Legis. 518 (2005) (imposing a notification obligation on "[a]ny person or business that conducts business" and defining a business as "a sole proprietorship, partnership, corporation, association, or other group, however organized and whether or not organized to operate at a profit, including a financial institution . . . or the parent or the subsidiary of a financial institution"); N.D. CENT. CODE § 51-30-02, N.D. Legis. 447 (2005) (applying to "[a]ny person that conducts business"). *But see* GA. CODE ANN. § 10-1-911(2) and § 10-1-912(a), Ga. Legis. 163 (2005) (limiting the obligation to "information brokers," who are defined as "any person or entity who, for monetary fees or dues, engages in whole or in part in the business of collecting, assembling, evaluating, compiling, reporting, transmitting, transferring, or communicating information concerning individuals for the primary purpose of furnishing personal information to nonaffiliated third parties," and not including "any governmental agency whose records are maintained primarily for traffic safety, law enforcement, or licensing purposes"); ME. REV. STAT. § 1348, Me. Legis. 379 (2005) (limiting the notification duty to information brokers). Some businesses may be exempt from state-law obligations imposed on businesses generally. *See, e.g.*, LA. REV. STAT. § 51:3076, La. Legis. 499 (2005) (exempting financial institutions that are subject to certain federal rules).

[171] *See* IND. CODE §§ 4-1-10-2 & 4-1-11-5, In. Legis. 91-2005 (2005) (limiting the notification obligation to state agencies, including state educational institutions); 2005 NEV. LAWS Ch. 486 (A.B. 334), § 4(1), Nv. Legis. 486 (2005) (slip copy) (imposing a duty on

notify data subjects that the security of their information has been (or may have been) violated.[174] Several of the states imposing notification obligations expressly authorize a civil action for damages.[175] In addition, Illinois allows a deceptive trade practices action,[176] which permits a

---

governmental agencies; separate provisions apply to persons "doing business" (2005 NEV. LAWS Ch. 486 (A.B. 334), § 6(1)(1), Nv. Legis. 486 (2005) (slip copy)) and "data collectors" (2005 Nevada Laws Ch. 485 (S.B. 347), § 24(1), Nv. Legis. 485 (2005) (slip copy)); R.I. GEN. LAWS. § 11-49.2-3 & 4, R.I. Legis. 05-225 (requiring that notification be provided by "[a]ny state agency or person that owns, maintains or licenses computerized data"; "person" is defined as "any individual, partnership association, corporation or joint venture") ; WASH. REV. CODE § 42.17(a)(1), Wa. Legis. 368 (2005) (imposing a notification on governmental agencies; other provisions place a similar obligation on "[a]ny person or business that conducts business (WASH. REV. CODE § 19, Wash. Legis. 368 (2005)).

[172] See 815 ILL. COMP. STAT. § 530/5 & 10(a), Il. Legis. 94-36 (2005) (imposing a notification obligation on a "data collector," which "may include, but is not limited to, government agencies, public and private universities, privately and publicly held corporations, financial institutions, retail operators, and any other entity that, for any purpose, handles, collects, disseminates, or otherwise deals with nonpublic personal information"); 2005 TENN. LAWS PUB. CH. 473 §§ 1(a)(2) and 1(b)(S.B. 2220), Tn. Legis. 473 (2005) (imposing a duty on an "information holder," which includes "any person or business that conducts business in this state, or any agency of the State of Tennessee or any of its political subdivisions").

[173] *See* DEL. CODE ANN. tit. 6, § 12B-101(2) and § 12B-102(a), De. Legis. 61 (2005) (imposing a notification obligation on a "commercial entity," "whether for profit or not-for-profit").

[174] *See, e.g.,* FLA. STAT. ANN. § 817.5681(1)(a), Fl. Legis. 2005-229 (imposing a notification obligation if personal information relating to a resident "was, or is reasonably believed to have been, acquired by an unauthorized person"); IND. CODE § 4-1-11-5, In. Legis. 91-2005 (2005) (similar).

[175] *See* CAL. CIV. CODE § 1798.84 (Westlaw current through Ch. 33 of 2005 Reg. Sess. urgency legislation & Gov. Reorg. Plan No. 2 of 2005) (stating that "[a] customer injured by a violation of this title may institute a civil action to recover damages"); LA. REV. STAT. § 51:3075, La. Legis. 499 (2005) (providing that "a civil action may be instituted to recover actual damages resulting from the failure to disclose in a timely manner to a person that there has been a breach of the security system resulting in the disclosure of a person's personal information"); 2005 NEV. LAWS Ch. 486 (A.B. 334), § 5 Slip Copy, Nv. Legis. 486 (2005) (slip copy) (providing that a "person who has suffered injury as the proximate result of a violation of this section may commence an action against the governmental agency for the recovery of his actual damages, costs and reasonable attorney's fees," subject to limitations): *id.* at § 6(7) (indicating that "[a] person who has suffered injury as the proximate result of a violation . . . may commence an action against the person doing business in this State for the recovery of his actual damages, costs and reasonable attorney's fees and, if the violation of this section was willful or intentional, for any punitive damages that the facts may warrant"); 2005 Tenn. Laws Pub. Ch. 473 § 1(h) (S.B. 2220), Tn. Legis. 473 (2005) (providing that "[a]ny customer of an information holder who is a person or business entity, but who is not an agency of the state or any political subdivision of the state, and who is injured by a violation of this section may institute a civil action to recover

"person who suffers actual damage . . . [to recover] actual economic damages or any other relief which the court deems proper,"[177] including "reasonable attorney's fees and costs."[178] In other states, the notification obligation is enforced by various means, such as administrative[179] or civil[180] fines or an action by the attorney general[181] to recover "direct economic damages"[182] or to remedy deceptive trade practices.[183]

In states not expressly providing for civil liability to data subjects, it may be possible to rely upon a notification statute that does not expressly create a private right of action as the basis

---

damages"); WASH. REV. CODE §§ 19(10)(a) & 42.17(10)(a), Wa. Legis. 368 (2005) (providing that "[a]ny customer injured by a violation of this section may institute a civil action to recover damages").

[176] *See* 815 ILL. COMP. STAT. § 530/20, Il. Legis. 94-36 (2005) (providing that "[a] violation . . . constitutes an unlawful practice under the Consumer Fraud and Deceptive Business Practices Act").

[177] 815 ILL. COMP. STAT. 505/10a(a) (Westlaw current through P.A. 94-89 of the 2005 Reg. Sess.).

[178] *Id.* at 815 ILL. COMP. STAT. 505/10a(c).

[179] *See* FLA. STAT. ANN. § 817.5681(1)(b), Fl. Legis. 2005-229 (providing that "[a]ny person required to make notification . . . who fails to do so within 45 days . . . is liable for an administrative fine not to exceed $500,000, as follows: 1. In the amount of $1,000 for each day the breach goes undisclosed for up to 30 days and, thereafter, $50,000 for each 30-day period or portion thereof for up to 180 days. 2. If notification is not made within 180 days, any person required to make notification under paragraph (a) who fails to do so is subject to an administrative fine of up to $500,000"). In Florida, "[t]he administrative sanctions for failure to notify provided in this subsection shall apply per breach and not per individual affected by the breach." *Id.* at § 817.5681(1)(c). Administrative sanctions generally do not apply against a "governmental agency or subdivision." *Id.* at § 817.5681(1)(d). *See also* MONT. CODE ANN. § 31-3-115(8)(2) & (3), Mt. Legis. 518 (2005) (treating violations as deceptive trade practices subject to injunctive relief and civil fines).

[180] *See* R.I. GEN. LAWS. § 11-49.2-6(a) *et seq.*, R.I. Legis. 05-225 (stating that "[e]ach violation of this chapter is a civil violation for which a penalty of not more than a hundred dollars ($100) per occurrence and not more than twenty-five thousand dollars ($25,000) may be adjudged against a defendant").

[181] *See* MINN. STAT. § 325E.61(6), Mn. Legis. 167 (2005) (providing for enforcement by the attorney general).

[182] *See* DEL. CODE ANN. tit. 6, § 12B-104, De. Legis. 61 (2005) (providing that "the Attorney General may bring an action in law or equity to . . . ensure proper compliance with this chapter or to recover direct economic damages resulting from a violation, or both").

[183] *See* 2005 CONN. LEGIS. SERV. P.A. 05-148 § 3(g) (S.S.B. 650), Ct. Legis. P.A. 05-148 (as apparently the sole remedy, providing that "[f]ailure to comply with the requirements of this section shall constitute an unfair trade practice . . . and shall be enforced by the Attorney General"). *See also* 815 ILL. COMP. STAT. 505/3 *et seq*. (Westlaw current through P.A. 94-89 of the 2005 Reg. Sess.) (describing the powers of the Illinois Attorney General).

for a suit alleging negligence *per se*.[184] State security breach notification laws, unlike the federal GLBA and related regulations discussed in Part II-B-1, may be found to be sufficiently specific to avoid allegations that they are too vague to set the standard of care. The laws require prompt action and typically spell out in detail how notification is to be given.[185] The laws do, however, allow certain variations.

The state notification statutes often permit database possessors to adopt their own notification procedures that comply with the notice and timing requirements of the statute.[186] They also allow for a delay in notification to accommodate the needs of law enforcement[187] or other important considerations. For example, the Illinois Personal Information Protection Act requires that "notification shall be made in the most expedient time possible and without unreasonable delay, *consistent with any measures necessary to determine the scope of the breach and restore the reasonable integrity, security, and confidentiality of the data system*."[188] However, this type of language does not question whether there is a duty, but simply allows for a nuanced analysis of whether there has been a breach.

More importantly, some of the security breach notification laws create unlikelihood-of-harm exceptions to the disclosure obligation. For example, the Connecticut law states that "notification shall not be required if, after an appropriate investigation and consultation with relevant federal, state and local agencies responsible for law enforcement, the person reasonably determines that the breach will not likely result in harm to the individuals whose personal information has been acquired and accessed."[189] The Florida law requires such a determination to "be documented in writing and the documentation must be maintained for 5 years."[190] These

---

[184] *See* Part II-B, *supra* (discussing general principles of negligence *per se*).

[185] *See, e.g.*, ARK. CODE ANN. § 4-110-105, Ar. Legis. 1526 (2005) (detailing the acceptability of various methods of providing notice, including written notice, e-mail notice, and types of "substitute notice").

[186] For example, the Delaware law provides that "an individual or a commercial entity that maintains its own notice procedures as part of an information security policy for the treatment of personal information, and whose procedures are otherwise consistent with the timing requirements of this chapter is deemed to be in compliance with the notice requirements of this chapter if the individual or the commercial entity notifies affected Delaware residents in accordance with its policies in the event of a breach of security of the system." DEL. CODE ANN. tit. 6, § 12B-103(a), De. Legis. 61 (2005). *See also* GA. CODE ANN. § 10-1-911(3), Ga. Legis. 163 (2005) (similar).

[187] *See, e.g.*, GA. CODE ANN. § 10-1-912(c), Ga. Legis. 163 (2005) (providing that notification "may be delayed if a law enforcement agency determines that the notification will compromise a criminal investigation" and "shall be made after the law enforcement agency determines that it will not compromise the investigation").

[188] 815 ILL. COMP. STAT. § 530/10, Il. Legis. 94-36 (2005) (emphasis added).

[189] 2005 CONN. LEGIS. SERV. P.A. 05-148 § 3(b) (S.S.B. 650), Ct. Legis. P.A. 05-148.

[190] FLA. STAT. ANN. § 817.5681(10)(a), Fl. Legis. 2005-229. "Any person [who] . . . fails to maintain the documentation for the full 5 years as required in this subsection is liable for an administrative fine in the amount of up to $50,000 for such failure." *Id.* at § 817.5681(10)(b).

types of exceptions limit the utility of a negligence *per se* analysis in some states. Under such a law, a defendant's reasonable determination that there was no likelihood of harm would presumably mean either that there was no violation of the statute as a result of non-disclosure of a security breach or that there was an excuse for any violation that occurred.[191] Either finding would be fatal to a negligence *per se* action.

Some state notification statutes not expressly providing for civil liability, such as the Maine Notice of Risk to Personal Data Act,[192] appear to leave room for courts to entertain negligence *per se* actions by ruling out arguments that statutorily created penalties[193] are intended to be the sole measure of a database possessor's obligations.[194] The Maine act states that "rights and remedies available under . . . [the statute] are cumulative and do not affect or prevent rights and remedies available under federal or state law"[195]

At the federal level, legislation has been introduced, but not yet adopted, that would "require Federal agencies, and persons engaged in interstate commerce, in possession of electronic data containing personal information, to disclose any unauthorized acquisition of such information."[196] That bill, introduced by Senator Diane Feinstein, would pre-empt inconsistent state legislation, but does not expressly provide that adversely affected data subjects can maintain a civil action to recover damages.[197] Another bill, proposed by Senator Arlan Spector, would subject businesses maintaining records relating to 10,000 or more persons to certain data protection and breach notification requirements and, among other enforcement mechanisms, would allow a state attorney general to maintain an action in federal court for "damages in the sum of actual damages, restitution, or other compensation on behalf of affected residents of the State; and . . . punitive damages, if the violation is willful or intentional."[198]

---

[191] *See* RESTATEMENT, THIRD, OF TORTS: LIABILITY FOR PHYSICAL HARM § 15 (Proposed Final Draft 2005) (discussing the role of excuse in negligence *per se*).

[192] ME. REV. STAT. § 1346 *et seq.*, Me. Legis. 379 (2005).

[193] Maine provides that a violation may result in "A. A fine of not more than $500 per violation, up to a maximum of $2,500 for each day the information broker is in violation of this chapter; B. Equitable relief; or C. Enjoinment from further violations." ME. REV. STAT. § 1349(1), Me. Legis. 379 (2005).

[194] *See also* N.D. CENT. CODE § 51-30-07, N.D. Legis. 447 (2005) (providing that the "attorney general may enforce this chapter," but that the "remedies, duties, prohibitions, and penalties of this chapter are not exclusive and are in addition to all other causes of action, remedies, and penalties . . . provided by law").

[195] ME. REV. STAT. § 1349(3), Me. Legis. 379 (2005).

[196] S. 115, 109th Cong. (2005), 2005 Cong. U.S. S 115.

[197] *Id.* at § 3(b)(3) & 5 (stating that "[t]he rights and remedies available under this subsection are cumulative and shall not affect any other rights and remedies available under law").

[198] S. 1332, 109th Cong. (2005), 2005 Cong. U.S. S. 1332, § 401 *et seq*.

B. Basic Tort Principles

1. General Duty or Limited Duty

Part II-C discussed how general tort principles and policies can be marshaled to support judicial recognition of a duty *to protect* database information. Many of those same arguments–particularly the reasoning relating to foreseeability of danger, opportunity to prevent harm, relationship between the parties (at least in business contexts), deterrence of future losses, desirable community consequences, and the availability of insurance–have equal application to the question of whether a database possessor has a duty *to disclose* intrusion to data subjects. Those policies favor judicial recognition of a notification duty. However, whether the burden that would be placed on the defendant would be too heavy to bear requires special consideration since the costs of providing notice will obviously differ from the costs of protecting a computer database.

Depending on the number of affected data subjects, the costs of notification might be substantial. Some breaches of security involve a risk to tens or hundreds of thousands of persons.[199] Notifying each of the affected individuals separately might be difficult, time-consuming, and labor intensive. In addition, unlike the costs of database protection, the expense of notification does not directly[200] benefit the database possessor. Indeed, disclosure of the breach may precipitate adverse publicity and loss of business.

The states that have passed security breach notification laws have shown how the burden imposed on database possessors can be minimized, in some contexts, through use of alternate modes of notification.[201] The same type of alternatives–which allow for aggregate methods of communication when personal notice would be too expensive or otherwise infeasible–should be taken into account in determining whether a common-law notification duty should be imposed and, if so, whether that duty has been breached.

A key question in determining whether notification should be required is whether

---

[199] *See* note 9, *supra*.

[200] However, the defendant may indirectly benefit, such as by protecting its reputation through candor.

[201] *See, e.g.*, DEL. CODE ANN. tit. 6, § 12B-101(4), De. Legis. 61 (2005) (providing that "'notice' means: (i) written notice; (ii) telephonic notice; (iii) electronic notice, if the notice provided is consistent with . . . [certain federal laws]; or (iv) substitute notice, if the individual or the commercial entity required to provide notice demonstrates that the cost of providing notice will exceed $75,000, or that the affected class of Delaware residents to be notified exceeds 100,000 residents, or that the individual or the commercial entity does not have sufficient contact information to provide notice. Substitute notice consists of all of the following: a. e-mail notice . . .; and b. conspicuous posting of the notice on the Web site page of the individual or the commercial entity if the individual or the commercial entity maintains one; and c. notice to major statewide media").

disclosure of the breach would be useful[202] or futile.[203] If there is nothing a data subject could do to protect his or her own interests following an intrusion into data security, there would be little reason to require notification. However, it is indeed possible for individuals to act to protect themselves from financial and physical harm that might be caused by persons with unauthorized access to their data.[204] The federal Fair and Accurate Transactions Act of 2003 (FACTA)[205] allows a consumer to place a "fraud alert"[206] in his or her files with credit reporting agencies. Certain state laws also enable a consumer to place a "security freeze" on his or her credit report, which "prohibits the consumer reporting agency from releasing the consumer's credit report or any information from it without the express authorization of the consumer."[207] Some state laws permit victims of information security breaches to obtain a court order declaring the individual a victim of identity theft.[208] Such a declaration can aid the data subject in dealing with law enforcement authorities or businesses. A consumer can also monitor his or her credit card and bank accounts more closely for evidence of unauthorized transactions or pay a monthly service fee to a company which tracks three national credit reporting companies on a daily basis and advises subscribers of key changes to their data (such as new applications for credit by someone using the subscriber's name and identity).[209] As to physical harm, a person who has been warned of data intrusion can exercise greater caution for personal safety, if the facts so warrant.[210]

---

[202] RESTATEMENT, THIRD, OF TORTS: LIABILITY FOR PHYSICAL HARM § 18 cmt. b (Proposed Final Draft 2005) (stating that "[i]n some situations a warning is desirable because it is effective in reducing the likelihood of an accident. Yet in other situations a warning is appropriate mainly because it reduces the likely severity of the injuries that such an accident might occasion").

[203] RESTATEMENT, THIRD, OF TORTS: LIABILITY FOR PHYSICAL HARM § 18 cmt. b (Proposed Final Draft 2005) (indicating that "in some situations, however, there is little or nothing a potential victim can do even if given a warning. For example, if a golfer's errant shot heads in the direction of a freeway next to the golf course, it would be pointless for the golfer to give a 'fore' warning to motorists on the freeway").

[204] *Cf.* FTC website, *supra* note 5 (discussing what to do if you think your identity has been stolen).

[205] P.L. No. 108-159 (2003) (codified in scattered sections of 15 and 20 U.S.C.).

[206] 15 U.S.C. § 1681c-1 (current through P.L. 109-33, Jul. 12, 2005).

[207] 2005 Wash. Legis. Serv. Ch. 342 § 1(1) (S.B. 5418), Wash. Legis. 342 (2005). "The consumer reporting agency . . . shall provide the consumer with a unique personal identification number or password to be used by the consumer when providing authorization for the release of his or her credit report for a specific party or period of time." *Id.* at § 1(4). *See also* 2005 CONN. LEGIS. SERV. P.A. 05-148 § 2 (S.S.B. 650), Ct. Legis. P.A. 05-148 (detailing security freeze procedures).

[208] *See* TEX. BUS. & COM. CODE § 48.202, Tx. Legis. 294 (2005) (detailing process).

[209] *See* Kathleen Pender, *Credit Reports - Free for All*, SAN FRANCISCO CHRON., Tues. Nov. 30, 2004 (describing Experian's credit-monitoring product, called Triple Alert, which provides customers with same-day notification anytime someone seeks credit in their name).

[210] *But see* Hayes v. California, 113 Cal. Rptr. 599, 602 (Cal. 1974) (holding that there was no duty to warn students of the risk of an attack on the beach at night because "the public is aware of the incidence of violent crime, particularly in unlit and little used places" and "it would

In many circumstances, American tort law has imposed liability for failure to warn.[211] Indeed, courts have sometimes held that there is a duty to warn even when there is no duty to do anything else. For example, in many states that still follow the traditional categories relating to premises liability–trespasser, licensee, and invitee–the only duty a possessor of land owes to a licensee is to warn of dangers of which the possessor is aware.[212] Similarly, in some states, essentially the only duty of a mental health professional who knows that his or her patient poses a risk of harm to a third person is to warn the third person (or authorities) of the danger.[213] Consequently, it might reasonably be urged that even if a state holds that there is no duty to protect databases from intrusion, there should at least be a duty to provide notice when the security of the database has been breached.[214]

There is an important question as to how specific the notice should be that informs data

---

serve little purpose . . . to further remind the public of this unfortunate circumstance in society").

[211] "The range of defendant conduct that can give rise to the obligation to warn is so broad as to make clear that the failure to warn is a basic form of negligence." RESTATEMENT, THIRD, OF TORTS: LIABILITY FOR PHYSICAL HARM § 18 cmt. a (Proposed Final Draft 2005) (offering diverse examples). *See also* RESTATEMENT, THIRD, OF TORTS: PRODUCTS LIABILITY § 2(c) (1998) (discussing product liability based on failure to warn); *id*. at § 10 (providing that "[o]ne engaged in the business of selling . . . products is subject to liability for harm . . . caused by the seller's failure to provide a warning after the time of sale . . . if a reasonable person in the seller's position would provide such a warning").

[212] *See* RESTATEMENT, SECOND, OF TORTS § 342 cmt. d (1965) (stating that "the licensee . . . is entitled to expect nothing more than a disclosure of the conditions which he will meet if he . . . enters, in so far as those conditions are known to the giver of the privilege").

[213] *See* RESTATEMENT, THIRD, OF TORTS: LIABILITY FOR PHYSICAL HARM § 41 Reporter's Note to cmt. g (Proposed Final Draft 2005) (stating that in "*Tarasoff*" cases, "[s]ome courts have declined to adopt a duty beyond that of warning. A substantial number of courts, and legislatures enacting statutes, limit the duty to warning the potential victim").

[214] If a duty to warn is imposed as a matter of common law principles, there are many open questions relating to the method for conveying the warning and the specificity of the message. In the absence of a governing statute, whether the database possessor acted reasonably will be determined on a case by case basis. However, attorneys advising clients on what they must do to avoid liability might do well to keep in mind that the Guidance states:

> If the institution determines that misuse of its information about a customer has occurred or is reasonably possible, it should notify the affected customer as soon as possible. Customer notice may be delayed if an appropriate law enforcement agency determines that notification will interfere with a criminal investigation and provides the institution with a written request for the delay. However, the institution should notify its customers as soon as notification will no longer interfere with the investigation.

Id.

subjects that their data has been accessed. In this regard, the federal Interagency Guidance[215] for financial institutions offers an informative, pro-consumer perspective. The Interagency Guidance states:

> Customer notice should be given in a clear and conspicuous manner. The notice should describe the incident in general terms and the type of customer information that was the subject of unauthorized access or use. It also should generally describe what the institution has done to protect the customers' information from further unauthorized access. In addition, it should include a telephone number that customers can call for further information and assistance. The notice also should remind customers of the need to remain vigilant over the next twelve to twenty-four months, and to promptly report incidents of suspected identity theft to the institution.[216]

---

[215] *See* Supplement A to Appendix B to Part 30 Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice 12 CFR Pt. 30, App. B (Westlaw current through July 1, 2005) (hereinafter "Interagency Guidance") (setting forth guidance jointly issued by the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, the Office of the Comptroller of the Currency, and the Office of Thrift Supervision interpreting the GLBA and related provisions). The Guidance opines that financial institutions have a duty to notify customers of a breach of data security. *See id*. (providing that "[w]here an incident of unauthorized access to customer information involves customer information systems maintained by an institution's service providers, it is the responsibility of the financial institution to notify the institution's customers and regulator").

[216] Interagency Guidance, *supra* note 215. More specifically, the document provides:

> The notice should include the following additional items, when appropriate:
>
> a. A recommendation that the customer review account statements and immediately report any suspicious activity to the institution;
>
> b. A description of fraud alerts and an explanation of how the customer may place a fraud alert in the customer's consumer reports to put the customer's creditors on notice that the customer may be a victim of fraud;
>
> c. A recommendation that the customer periodically obtain credit reports from each nationwide credit reporting agency and have information relating to fraudulent transactions deleted;
>
> d. An explanation of how the customer may obtain a credit report free of charge; and
>
> e. Information about the availability of the FTC's online guidance regarding steps a consumer can take to protect against identity theft. The notice should encourage the customer to report any incidents of identity theft to the FTC, and should provide the FTC's Web site address and toll-free telephone number that customers may use to obtain the identity theft guidance and report suspected incidents of identity theft.

Id. The Interagency Guidance adds that:

> Customer notice should be delivered in any manner designed to ensure that a customer can reasonably be expected to receive it. For example, the institution may choose to contact all customers affected by telephone or by mail, or by electronic mail for those customers for whom it has a valid e-mail address and who have agreed to

2. The Obligation to Correct Previous Statements

There is a duty to update previous statements that were intended to induce reliance and which, though true when made, have become false or misleading as a result of subsequent developments.[217] The duty extends until the recipient of the information is no longer able to protect his or her own interests by foregoing reliance on the now-erroneous representation of the fact.[218] The purpose of the rule is to avoid deception that causes harm.

The operation of this rule can be illustrated by a case from another context, *McGrath v. Zenith Radio Corp.*[219] In that case, the defendants had told the plaintiff executive that he was the "heir apparent" to the presidency of a soon-to-be-acquired subsidiary. However, before the executive released his shares of stock and options to facilitate the acquisition, the defendants learned that there were serious doubts as to whether the plaintiff would ever become president. They did not disclose those developments. In an opinion by Chief Judge Thomas E. Fairchild, the Seventh Circuit upheld a judgment in favor of the executive, for in releasing his options and selling his shares he had relied on the assurances that others thought he would be the new corporate head and was never advised to the contrary. "The making of the original statements, the discovery of their falsehood, and the failure to correct them before plaintiff relied on them were 'elements in a continuing course of conduct' capable of establishing fraud."[220]

---

receive communications electronically.

Id.

[217] *See* Sharff v. Pioneer Financial Service, Inc., 1993 W.L. 87718, *6-*7 (N.D. Ill) (recognizing the rule and holding there was a question of fact as to whether the defendant failed to correct a representation that the plaintiff would be given a performance review); Stevens v. Marco, 305 P.2d 669, 683 (Cal. Dist. Ct. App. 1957) (citations omitted) (stating that "one who learns that his statements, even if thought to be true when made, have become false through a change in circumstances, has the duty, before his statements are acted upon, to disclose the new conditions to the party relying on his original representations"); St. Joseph Hosp. v. Corbetta Constr. Co., 316 N.E.2d 51, 71 (Ill. App. Ct.1974) (stating that "where one has made a statement which at that time is true but subsequently acquires new information which makes it untrue or misleading, he must disclose such information to anyone whom he knows to be acting on the basis of the original statement–or be guilty of fraud or deceit"); Mahan v. Greenwood, 108 S.W.3d 467, 494 (Tex. App. 2003) (holding that an attorney had a duty to correct any misimpressions caused by his earlier statements); 2 FOWLER V. HARPER *et al.*, THE LAW OF TORTS § 7.14, at 476 (2d ed. 1986). *See also* First Nat. Bk. of Elgin v. Nilles, 35 B.R. 409, 411 (D.C. Ill. 1983) (stating that "one who makes an incorrect statement he has reason to believe another is relying upon is under a duty to correct it").

[218] *See* RESTATEMENT, SECOND, OF TORTS § 551 cmt. h (1977) (providing that "[o]ne who, having made a representation which when made was true or believed to be so, remains silent after he has learned that it is untrue and that the person to whom it is made *is relying* upon it in a transaction with him, is morally and legally in the same position as if he knew that his statement was false when made") (emphasis added).

[219] 651 F.2d 458 (7th Cir. 1981) (applying California law).

[220] 651 F.2d at 468.

Similarly, it might be argued that when businesses tell their customers–through advertisements, websites, or published privacy policies[221]–that their personal data is secure, but then learn information to the contrary, they have a duty to disclose those developments to their customers.[222] The customers have a choice as to whether to continue to their relationships with the businesses in question. There has been no irrevocable reliance by a customer, even though a business-customer relationship is already in progress. It is still possible to for the customer to act to protect his or her interests by terminating the relationship and doing business elsewhere.

It is important to note that in *McGrath* and similar cases, the defendants were not guilty of mere negligence, but of fraud. In fraud actions, economic losses are routinely recoverable,[223] except in a minority of states.[224] Consequently, if a duty to speak is imposed under this theory, the scope of liability may not be limited by the economic-loss rule, discussed below,[225] or by usual requirements of foreseeability.[226] In addition, "[e]motional harm damages are not ordinarily recoverable in a misrepresentation action,"[227] and thus the issues addressed in Part IV-B may be irrelevant under this theory of liability.

3. Conduct Creating a Continuing Risk of Physical Harm

It is well established that where a person's prior conduct creates a continuing risk of

---

[221] See notes 136 & 137, *supra*, and the accompanying text.

[222] *Cf.* ABA Business Law Section, Thomas J. Smedinghoff, *Trends in the Law of Information Security*, 2 CIPARETI No. 1 (Mar. 2005), at http://www.abanet.org/buslaw/committees/CL320010pub/newsletter/0006/ (last visited July 25, 2005) (stating that "government enforcement agencies such as the Federal Trade Commission (FTC) have actively pursued companies for 'deceptive' trade practices whenever the information security representations they voluntarily make to the public do not match their actual security practices").

[223] *See* ROBERT L. DUNN, RECOVERY OF DAMAGES FOR FRAUD 20 (3d. ed. 2003) (indicating that "dozens of cases are decided every year awarding economic loss damages for fraud"); *id.* at 24-26 (discussing cases holding that the economic-loss rule does not apply to misrepresentation claims). *See also id.* at 20 (stating that "[i]f the economic-loss rule is held to bar damages for misrepresentation, the courts are saying that there is no difference between deliberate lying, that is, common-law fraud, and innocent sales of goods that happen not to conform to the contract").

[224] *See id.* at 20 (stating that "only a minority of states and a few federal courts have held the economic loss rule applicable to fraud claims").

[225] *See* Part IV-A, *infra*.

[226] *See* DUNN, *supra* footnote 223, at 18 (stating that "[t]here is no policy behind limiting the damages recoverable against one who defrauds another to those damages that the party committing the fraud might have been able to foresee at the time he or she made the misrepresentation").

[227] DAN B. DOBBS, THE LAW OF TORTS 1381 (2000) (hereinafter "TORTS". *But see* DUNN, *supra* footnote 223, at 170 (stating that "courts have been divided sharply in recent years as to whether emotional distress is a recoverable element of damages for fraud).

physical harm there is a duty to render assistance to keep the harm from occurring or mitigate adverse consequences.[228] This duty exists even if the prior conduct was not tortious.[229] Thus, a driver involved in an auto accident must stop to render assistance, regardless of whether he or she was at fault for the collision.[230] Likewise, a landlord who sprays an apartment, carelessly or not, with a pesticide that makes a tenant ill is obliged to disclose its contents, in response to a request, to aid medical care of the tenant.[231]

The harm caused by intrusions into computerized personal data typically is more economic than physical in nature.[232] Yet misuse of improperly accessed personal data can result in a physical attack on a data subject or physical harm to property. Hacking of a newspaper's records, for example, may reveal when a customer's paper will be on "vacation hold" and thereby lead to a burglary while the customer is away on vacation.

In *Remsburg v. Docusearch, Inc.*,[233] an Internet-based investigation service obtained a woman's workplace address not through hacking, but by placing a pretext phone call and duping her into revealing her employment information. The party who purchased the data from the service then went to the workplace and killed the woman. The court held that an information broker who sells data pertaining to a person owes a duty of care to that person when disclosing the information to a client. In cases like *Remsburg*, where personal data leads to physical harm, information might be obtained by hacking personal data in possession of a third party, thus potentially bringing the increased-risk-of-harm rule into play.

As articulated by the new Restatement, the existence of a duty of reasonable care under

---

[228] *See* RESTATEMENT, THIRD, OF TORTS: LIABILITY FOR PHYSICAL HARM § 39 (Proposed Final Draft No. 1 2005) (providing that "[w]hen an actor's prior conduct, even though not tortious, creates a continuing risk of physical harm of a type characteristic of the conduct, the actor has a duty to exercise reasonable care to prevent or minimize the harm"); *see also* RESTATEMENT, SECOND, OF TORTS § 321 (1965) (stating that "(1) If the actor does an act, and subsequently realizes or should realize that it has created an unreasonable risk of causing physical harm to another, he is under a duty to exercise reasonable care to prevent the risk from taking effect. (2) The rule stated in Subsection (1) applies even though at the time of the act the actor has no reason to believe that it will involve such a risk").

[229] *See* RESTATEMENT, THIRD, OF TORTS: LIABILITY FOR PHYSICAL HARM § 39 (Proposed Final Draft No. 1 2005) ("even though not tortious").

[230] *Cf.* RESTATEMENT, SECOND, OF TORTS § 321 illus. 3 (1965) (indicating that a driver involved in a skidding accident has a duty to warn on-coming drivers).

[231] *See* La Raia v. Superior Ct., 722 P.2d 286, 290 (Ariz. 1986) (stating that "[h]aving caused or contributed to plaintiff's poisoning, defendant was under a duty to act reasonably to mitigate the resulting harm").

[232] *See* Rustad & Koenig, *supra* note 14, at 93 (noting that "[t]he predominant injury in a cybertort case is a financial loss").

[233] 816 A.2d 1001 (N.H. 2003).

this rule depends upon (1) "prior conduct,"[234] which (2) "creates a continuing risk of physical harm,"[235] that is (3) "of a type characteristic of the conduct."[236] Where improperly accessed computerized data is used to cause physical harm, the database possessor's "prior conduct" is the maintenance of the information in a form where one of the foreseeable risks is unauthorized intrusion. That conduct may qualify as tortious (if the database possessor has been careless in safeguarding the data) or it may be innocent (if the database possessor has exercised reasonable care or was under no duty to do so). It makes no difference. The loss of the data creates some risk of physical harm to data subjects–often not a great risk, but not a negligible risk either. If the conduct and risk requirements are satisfied, the question is then whether, if physical harm occurs, it is a type of harm "characteristic of the conduct." Concerning this requirement, the Restatement commentary offers guidance:

> The conduct must . . . be sufficiently connected with the potential for later harm that imposing a duty to prevent or mitigate the harm is appropriate. . . . [I]t is unfair to impose this duty when the actor's conduct has not generally increased the risk of harm . . . or is quite removed from the risks that pose harm to the other . . . .[237]

Whether a defendant's practices in maintaining a database have sufficiently "increased the risk of harm" to the data subject, or are too far "removed" from those risks, are matters that will depend heavily on the specific facts. In some cases, the connection between the defendant's role in the loss of the information and the resulting threatened physical harm may be sufficiently great as to give rise to a duty to warn the data subject that the security of his or her personal information has been breached. This theory of liability is only applicable in cases where the data subject suffers physical harm. However, if personal injuries are inflicted, the amount of damages may be great.

C. Fiduciary Duty of Candor

A fiduciary relationship imposes a duty of candor. The fiduciary must exercise reasonable care to reveal all material information to the person to whom the duty is owed.[238] Indeed, when the interests of the fiduciary and the beneficiary are adversely aligned, fiduciary principles may require something more than reasonable care, perhaps a degree of

---

[234] RESTATEMENT, THIRD, OF TORTS: LIABILITY FOR PHYSICAL HARM § 39 (Proposed Final Draft No. 1 2005).

[235] *Id.*

[236] *Id.*

[237] RESTATEMENT, THIRD, OF TORTS: LIABILITY FOR PHYSICAL HARM § 39 cmt. c (Proposed Final Draft No. 1 2005).

[238] *Cf.* Nicola W. Palmieri, *Good Faith Disclosures Required During Pre-Contractual Negotiations*, 24 SETON HALL L. REV. 70, 127 (1993) (stating that a "party who owes . . . [a] confidential or fiduciary duty has an obligation to divulge or disclose during negotiations all material facts concerning the transaction within his knowledge").

forthcomingness that approximates "absolute and perfect candor."[239]

If a database possessor owes fiduciary obligations to a data subject (as in the case of an attorney and client), it seems clear that the possessor must disclose information relating to a breach of database security. The interests of the fiduciary and the data subject are in potential conflict because there are important questions as to whether the possessor may be held responsible for the loss of the data. The law requires the fiduciary to subordinate his or her personal interests to the interests of the data subject.[240] Non-disclosure would be inconsistent with those heavy obligations.

This theory of notification duty, like the earlier discussion of whether fiduciaries have a duty to safeguard computerized personal information,[241] has limited applicability. It does not govern the general run of commercial cases. However, it may be of great importance in cases involving lawyers, physicians, and other fiduciaries who maintain computerized records containing personal data relating to clients, patients, and beneficiaries.

IV. Limiting Cybersecurity Tort Liability

Assuming that a database possessor has breached a duty to protect personal data or reveal information of unauthorized access to computerized information, how far should tort liability extend? Should an affected data subject be able to recover as damages amounts for economic losses or emotional distress resulting from the breach? If these or other substantial damages are ordinarily recoverable, is there anything the defendant database possessor can do, between the time of the breach and the moment of harm, to minimize its exposure to tort liability? These issues are considered in the following subparts.

A. The Economic-Loss Rule

The economic-loss rule is an "obscure,"[242] but important, legal doctrine which holds that a plaintiff may not recover economic losses resulting from negligence that are unaccompanied

---

[239] *Cf.* Johnson, *Candor*, *supra* note 143, at 771 (stating that in legal representation a "duty of 'absolute and perfect candor' applies most forcefully in instances where the interest of the attorney and client are adverse").

[240] There are difficult questions as to how far a fiduciary's duty of candor extends. The duty is limited by considerations relating to scope of the relationship, materiality, prior knowledge of the information, competing obligations to others, consent, and likelihood of harm. *See* Johnson, *Candor*, *supra* note 143, at 778-92. For a discussion of whether a lawyer must tell a client that the lawyer may have committed malpractice, see *id.* at 773 & n.182.

[241] *See* Part II-D, *supra*.

[242] John J. Laubmeier, *Demystifying Wisconsin's Economic Loss Doctrine*, 2005 WIS. L. REV. 225, 225 (noting that "the application of the doctrine is a constantly developing area of law, which may not be fully understood by judges, lawyers, or the public at large").

by physical damage to the plaintiff's person or property.[243] Obviously, if the economic-loss rule applies to cybersecurity cases, it has the potential to greatly limit the scope of recoverable damages.[244] Consequently, it is important to understand the policies underlying the rule and the precise nature of its restrictions. Viewed from the standpoint of public policy, the economic-loss rule serves three very different functions: avoidance of too broad a scope of liability; insistence that damages be proved with certainty; and definition of the doctrinal boundary between contract law and torts.

First, somewhat crudely, the economic-loss rule protects potential defendants from the risk of a disproportionately wide range of liability.[245] This is an important function, for acts of negligence often have broad adverse economic consequences. There would be no sensible stopping point to tort liability if a referee who negligently makes a bad call that eliminates a team from the playoffs were liable for the lost profits of merchants who sell team-related items[246] or if a person who causes an auto accident were responsible for all of the economic losses that result from the delays of persons tied up in traffic.[247] Not surprisingly, the Restatement provides, as a general rule, that there is no liability for negligent interference with contracts or economically promising relations.[248] According to Professor Jay M. Feinman:

---

[243] *See* Ann O'Brien, Note, *Limited Recovery Rule as a Dam: Preventing a Flood of Litigation for Negligent Infliction of Pure Economic Loss*, 31 ARIZ. L. REV. 959, 959 (1989) (stating a similar definition). *See also* Dunn, *supra* footnote 223, at 19 (stating that "[i]n the last ten years or so, most courts have held . . . economic loss unaccompanied by property damage or personal injury not be recoverable in an action alleging negligence or strict liability in the manufacture of a product").

[244] *See* Rustad, *supra* note 2, 6, at 113 (opining that "[t]he economic loss rule adopted by most courts is a barrier to tort recovery for Internet-related security breaches").

[245] *See* JAY M. FEINMAN, ECONOMIC NEGLIGENCE: LIABILITY OF PROFESSIONALS AND BUSINESSES TO THIRD PARTIES FOR ECONOMIC LOSS 12 (1995) (hereinafter "ECONOMIC NEGLIGENCE") (stating that a "distinctive feature of economic negligence cases is the fear of indeterminate liability" meaning both "indeterminacy of the number of potential plaintiffs . . . and the size of their claims"); *id.* at § 1.3.2 (discussing the threat of indeterminate liability).

[246] *See* Bain v. Gillispie, 357 N.W.2d 47 (Iowa App. 1984) (holding that injury to novelty store owners' business interests was not a reasonably foreseeable result of a college basketball referee's call which had effect of eliminating the local team from the conference championship; no liability for "malpractice").

[247] *See* Petition of Kinsman Transit Co., 388 F.2d 821 (2d Cir. 1968) (denying recovery to persons who incurred additional shipping costs when a bridge collapsed as a result of multiple acts of negligence).

[248] *See* RESTATEMENT, SECOND, OF TORTS § 766C (1977) (stating that "[o]ne is not liable to another for pecuniary harm not deriving from physical harm to the other, if that harm results from the actor's negligently (a) causing a third person not to perform a contract with the other, or (b) interfering with the other's performance of his contract or making the performance more expensive or burdensome, or (c) interfering with the other's acquiring a contractual relation with a third person"); *id.* at cmt a (opining that courts "apparently have been influenced by . . . the fear of an undue burden upon the defendant's freedom of action, the probable disproportion

> [I]ndeterminacy [of the scope of liability in economic negligence cases] is a concern not in and of itself but through its relation to fundamental tort policies. When liability is indeterminate, arguably the deterrence, loss distribution, and fairness policies are undermined.[249]

Second, lost economic opportunities are often not readily susceptible to precise calculation.[250] Yet, the law insists that damages must be proved with reasonable certainty. The economic-loss rule, by ruling out litigation in a huge range of cases (suits where there is no personal injury or property damage), helps to ensure (again somewhat crudely)[251] that compensation is not awarded for amounts that are speculative.[252] In the process of doing so, the economic-loss rule promotes judicious use of limited judicial resources. Those scarce assets are not squandered on the burdensome, and perhaps dubious, task of trying to quantify endless economic losses that may, in truth, not be provable with reasonable precision.[253]

---

between the large damages that might be recovered and the extent of the defendant's fault, and perhaps in some cases the difficulty of determining whether the interference has in fact resulted from the negligent conduct").

[249] FEINMAN, ECONOMIC NEGLIGENCE, *supra* footnote 245, at 18.

[250] *Cf.* J'Aire Corp. v. Gregory, 157 Cal. Rptr. 407, 410 (Cal. 1979) (stating that "[t]he chief dangers . . . in allowing recovery for negligent interference with prospective economic advantage are the possibility of excessive liability, the creation of an undue burden on freedom of action, the possibility of fraudulent or collusive claims and the *often speculative nature of damages*"; emphasis added).

[251] This is not the only occasion when the law employs a rather blunt rule to limit the scope of tort liability. In some states, for example, there is no liability for negligent infliction of emotional distress unless the plaintiff suffers some form of physical impact or physical consequences. *See* Brown v. Matthews Mortuary, Inc., 801 P.2d 37 (Idaho 1990) (holding that a son could not recover for distress allegedly resulting from mortuary's negligent loss of the cremated remains of his father absent physical manifestations of injury); Bader v. Johnson, 732 N.E.2d 1212, 1221-22 (Ind. 2000) (indicating that Indiana continues to adhere to a modified impact rule).

[252] *But see* DUNN, *supra* footnote 223, at 18-19 (stating that "[t]he rule that precludes recovery of uncertain and speculative damages applies where the *fact* of damages is uncertain, not where the *amount* is uncertain. . . . Computation of the amount is for the trier of fact").

[253] *See* JOHNSON & GUNN, *supra* note 33, at 7-9 (stating that "[i]t has often been urged that . . . [t]ort law should be administratively convenient and efficient, and should avoid intractable inquiries. Only a limited amount of resources can be devoted to the administration of justice in any society. This principle holds that tort rules should be shaped so that the dollars spent on accident compensation are efficiently employed. Thus, legal standards should not be so complex or uncertain that their application entails an undue expenditure of judicial resources or imposes unnecessarily high litigation costs on parties. So, too, convenience and efficiency discourage the pursuit of what might be called intractable inquiries, matters where the facts are such that even after expenditure of considerable time and money, there is a substantial risk that an erroneous result will be reached").

Third and most importantly, the economic-loss rule marks the boundary line between contract law and tort law.[254] Delineating these two bodies of law is vital for otherwise there is a risk that "contract law would drown in a sea of tort."[255] The law of contracts has meaning only because entering into agreements has legal consequences. One of those consequences is that if a person makes a bad deal, he or she usually must suffer the result. This reality creates an incentive for contracting parties to exercise diligence to protect their own interests.[256] If a party who strikes a disadvantageous bargain could successfully complain that he or she should recover damages because the other side failed to exercise reasonable care to protect his or her interests, a great part of contract law would be rendered superfluous.

The best example of how the economic-loss rule distinguishes contract claims from torts is a case involving a defective product, *East River Steamship Corp. v. Transamerica Delaval*.[257] That suit, which eventually reached the nation's highest court, involved a defective component part of a turbine which damaged only the turbine itself. There was no harm to any person or to "other" property of the plaintiffs. The action sought damages in tort for the cost of repairs to the turbine and for lost profits because statutes of limitations had already barred contract claims. The Supreme Court, in an opinion by Justice Harry Blackmun, held that a manufacturer has no tort duty under negligence or strict liability to prevent a product from injuring itself. Those types of harm are merely economic losses that can be insured against or otherwise addressed by the parties while negotiating the contract. Only product defects that result in harm to property other than the product itself or in personal injury are cognizable under the law of torts. The law of warranty provides sufficient protection for the benefits of the bargain.

---

[254] *See* note 29, *supra*. *See also* FEINMAN, ECONOMIC NEGLIGENCE, *supra* footnote 245, at § 1.3.3 (discussing the protection of private ordering); Kevin J. Breer & Justin D. Pulikkan, *The Economic Loss Rule in Kansas and its Impact on Construction Cases*, 74-JUN J. KAN. B.A. 30, 31 (2005) (stating that "[t]he economic loss rule can be justified for three reasons: (1) it maintains a 'fundamental distinction between tort and contract law;' (2) it protects commercial party's freedom to 'allocate economic risk by contract;' and (3) it encourages 'the parties best situated to assess the risk of economic loss' and to 'assume, allocate, or insure against the risk'").

[255] East River Steamship Corp. v. Transamerica Delaval, 476 U.S. 858, 866 (1986) (citing G. GILMORE, THE DEATH OF CONTRACT 87-94 (1974)). *See generally* Vincent R. Johnson, *Liberating Progress and the Free Market from the Specter of Tort Liability*, 83 NW. U. L. REV. 1026, 1030 (1989) (stating that, according to one legal commentator, "ever-more-generous incarnations of tort law ascended to the throne of accident compensation following the decline of privity, the narrowing construction of disclaimers, and the widely heralded 'death of contract'").

[256] *See* JOHNSON & GUNN, *supra* note 33, at 9 (noting that it has often been urged that the law should be shaped to "promote individual responsibility" and to encourage persons "to employ available resources to protect their own interests, rather than depend on others to save them from harm").

[257] 476 U.S. 858 (1986). *See also* Glaub Jewelers, Inc. v. New York Daily News, 535 N.Y.S.2d 532 (N.Y.C. Civ. Ct. 1988) (holding that a newspaper that negligently failed to publish an advertisement for a business was not liable in tort for the business's lost sales).

With these three policy considerations in mind–scope of liability, certainty of damages, and delineation of contact-versus-tort–the question is then whether the economic-loss rule should apply to cybersecurity cases and, if so, what claims for damages might be barred. Answering those questions involves consideration of the types of economic losses that may arise in these cases, as well as the efficacy of contract law and the insurance market in addressing such losses. Unauthorized use of personal information can result in many types of harm. In cybersecurity cases where breaches of security result in identity theft, the losses include, but are not limited to: (1) out-of-pocket expenses incurred to restore a good credit rating; (2) personal time spent on that task; and (3) lost opportunities resulting from bad credit.

Focusing first on out-of-pocket losses,[258] there is little policy justification for denying recovery. Various estimates currently peg these costs in a typical case at between $800[259] and $1400.[260] Even though the amount out-of-pocket damages may vary from case to case, this element of damages is susceptible to proof with a high degree of certainty. The receipts are gathered, a list is made, and the sum is totaled. There is no reason relating to certainty of harm to deny compensation for amounts actually and reasonably spent on the task of restoring a good credit rating on the ground that out-of-pocket damages are speculative.

Nor does recovery of out-of-pocket costs present a case where the circle of liability needs to be tightly circumscribed to prevent legal responsibility from being extended too far. In many cases, there will be a business relationship between the database possessor and damaged data subject, and in other cases the relationship (presumably) will be sufficiently close that there was some legitimate reason for the defendant to maintain a database containing personal information about the plaintiff.[261] These are not situations where some "stranger" in the community (e.g., the vendor of the losing team's products[262] or the person tied up in traffic,[263] mentioned above) is seeking to recover damages. If a database possessor wishes to constrict the scope of potential liability, it may always do so by removing from its database the personal information of data subjects. But if it fails to do so, the courts should be reluctant to deny recovery of out-of-pocket losses to data subjects whose interests were imperiled by the database possessor's choice to maintain personal information in a form where one of the risks was unauthorized access.

If, with respect to out-of-pocket losses, scope of liability and uncertainty of damages are not significant considerations, the only question, so far as the economic-loss rule is concerned, is

---

[258] Presumably these costs would include items such as postage, phone calls, photocopying, gasoline, and the like, as well as the cost of obtaining court documentation that one is the victim of identity theft.

[259] *See Stop Thieves*, *supra* note 1, at 12 (stating that victims of identity theft "typically lose $800 and spend two years clearing their names").

[260] *See* Texas Bill Analysis, *supra* note 4.

[261] Indeed, if the database possessor had no legitimate reason for maintaining the personal information of the data subject, that itself might incline a court not to relieve the possessor of exposure to liability.

[262] *See* footnote 246, *supra,* and the accompanying text.

[263] *See* footnote 247, *supra,* and the accompanying text.

whether the boundary-line between contracts and torts creates a good reason for a court to say this is the type of loss that should be compensated only if there is a contractual obligation to do so. The answer to that question is "no."

There is an emerging consensus reflected in the recently passed state security breach notification statutes which suggests that rights relating to protection of personal data and notification of security breaches *are not* proper subjects for bargaining between the parties. Many of the state laws,[264] such as the Rhode Island Identity Theft Protection Act of 2005,[265] provide that a waiver of the rights they give data subjects is against public policy, and therefore void and unenforceable. If that is true, it makes little sense to say that a consumer should bargain and pay for the level of cybersecurity protection (and the right to sue for out-of-pocket damages) that he or she desires. Moreover, it is simply unrealistic to expect such bargaining to occur between individual consumers and the large corporations that play a pervasive role in modern life. Individuals often lack both commercial leverage[266] and the information necessary to assess the risks that they face. "[I]t would be entirely possible that despite good faith efforts and the expenditure of considerable funds, a customer would fail to obtain a fully accurate and complete picture of potential harms, with the result being an unintentional and undesired assumption of risk by the consumer."[267] Moreover, in light of the ubiquity of computerized databases, ordinary persons would have to devote a huge amount of energy to negotiating the parameters of data protection with every potential defendant, if contract law were the only solution to these types of problems. As a result, "[c]onsumers would spend an inordinate amount of resources on efforts to perform often duplicative, time-consuming tasks relating to assessment of the risks of injury and the need for economic protection."[268]

As an alternative to this sort of David-versus-an-army-of-Goliaths contractual model, a better paradigm is one that is structured so that compensation for foreseeable and necessary out-of-pocket losses is routinely recoverable from the tortfeasor. Compensation of out-of-pocket losses should not depend upon whether the data subject read the fine print in the defendant's privacy policy or bargained for a specific level of protection, but on the reasonableness of the

---

[264] *See* ARK. CODE ANN. § 4-110-107, *et seq*., Ar. Legis. 1526 (2005) (stating that "[a]ny waiver of a provision of this subchapter is contrary to public policy, void, and unenforceable"); CAL. CIV. CODE § 1798.84(a) (Westlaw current through Ch. 33 of 2005 Reg. Sess. urgency legislation & Gov. Reorg. Plan No. 2 of 2005) (similar); 815 ILL. COMP. STAT. § 530/15, Il. Legis. 94-36 (2005) (similar); MINN. STAT. § 325E.61(3), Mn. Legis. 167 (2005) (similar); 2005 Nevada Laws Ch. 485 (S.B. 347), § 27, Nv. Legis. 485 (2005) (slip copy) (similar); WASH. REV. CODE § 42.17(9), Wa. Legis. 368 (2005) (similar).

[265] R.I. GEN. LAWS. § 11-49.2-6(b) *et seq*., R.I. Legis. 05-225.

[266] *See* Johnson, *Liberating Progress*, *supra* note 255, at 1044 (discussing the "the inequalities of bargaining power which pervade many consumer transactions" and noting that "[p]urveyors of goods and services frequently employ standardized contracts which leave consumers little choice but to accept a deal as presented–including contractual terms which purport to limit the provider's liability to the consumer").

[267] Johnson, *Liberating Progress*, *supra* note 255, at 1042.

[268] Johnson, *Liberating Progress*, *supra* note 255, at 1042.

amounts spent to restore a good credit rating. This is a function that can be better performed by tort law than by contracts.[269] Moreover, the function is not one for which the insurance market has yet offered an adequate substitute. According to Consumer Reports, "ID theft insurance is typically not worth paying for."[270]

The preceding analysis of the propriety of out-of-pocket credit-repair damages can be profitably contrasted with requests for recovery of compensation for time spent restoring one's good credit or for opportunities lost as a result of a bad credit rating. Statistics show that victims of identity theft spend 600 hours on average[271] to restore their credit. Obviously, the harm suffered by these victims is tremendous. Yet it is easy to see why it would be difficult to value these lost hours. If plaintiff's time were compensated at his or her usual hourly rate of earnings in employment or a profession, the awards made to professionals, minimum-wage workers, and unemployed homemakers would vary widely–and perhaps without good reason. Similarly, if every victim were to receive the same amount for the value of lost time, how would that amount be set? Ensuring uniformity with respect to this element of damages is a task better committed to legislatures than to the multitude of fact finders who will preside over numerous tort claims.

The problems of compensating for the value of lost opportunities–such as the lost chance to buy a house, obtain a car loan, or open a cell-phone account–are also obvious. How does one prove precisely which opportunities were lost, and what they meant in economic terms to the plaintiff? In addition, there is a clear risk of imposing a range of liability that may be far too wide. Negligence requires only a momentary misstep, whether in the data protection arena or in other contexts. To say that a negligent database possessor should be liable to a broad class of persons for all of their lost opportunities (as well as out-of-pocket and perhaps other damages as well) would quickly pose a serious risk of liability disproportionate to fault.[272] All of this

---

[269] Under contract law, consequential damages are not recoverable unless they were specifically in the mind of the parties at the time the contract was entered into. *See* DAN B. DOBBS, LAW OF REMEDIES § 12.4(5) (2d ed. 1993) (discussing the "contemplation of the parties rule"). Consequently, it would be difficult to recover out-of-pocket credit-repair damages under a contractual theory of liability.

[270] *Stop Thieves*, *supra* note 1, at 12. "[P]olicies generally cover the expenses of cleaning up the crime, including attorney's fees, costs of mailing correspondence, and lost wages. They seldom cover the out-of-pocket loss to the victim. . . ." *Id.* at 14.

[271] *See* Texas Bill Analysis, *supra* note 4. *But see* McMahon, *supra* note 3, at 626 n.5 (2004) (citing a 175-hour figure).

[272] *See* JOHNSON & GUNN, supra note 33, at 7 (stating that "[t]he proportionality principle seeks to limit or refine application of the fault principle. In part, it holds that liability should not be levied on an individual tortfeasor, even if fault is shown, if doing so would expose the defendant to a burden that is disproportionately heavy or perhaps unlimited"). The proportionality principle is one of the most important forces in modern American tort law. To avoid imposition of disproportionate liability, courts and legislatures have: crafted limited-duty rules (*see* RESTATEMENT, THIRD, OF TORTS: LIABILITY FOR PHYSICAL HARM (BASIC PRINCIPLES) § 41 Cmt. g Reporters' Note (Proposed Final Draft No. 1, 2005) (discussed the sometimes-limited duties of mental-health professionals); imposed what amount to "standing to sue"

suggests that there is greater reason for courts to apply the economic-loss rule to bar claims for lost time and lost opportunities than to hold that out-of-pocket losses are not recoverable.

In any event, the economic-loss rule, as defined in most states, has important limits. First, it bars only claims for economic harm caused for negligence.[273] It therefore may be possible to avoid the rule by proving more culpable conduct, such as recklessness or intentional wrong-doing.[274] Second, the economic-loss rule is a common-law doctrine that does not preempt legislative provisions to the contrary. Liability for negligently caused economic harm may be actionable pursuant to statute. At least one state, Illinois,[275] expressly allows for recovery of economic losses in cybersecurity cases. Third, many types of harm caused by intrusion are not purely economic. Thus, damages for personal injury, property damage, and, perhaps, even emotional distress, are not barred by the rule. Fourth, some states show little enthusiasm for the economic-loss rule[276] and may determine that it does not apply to cybersecurity cases. Finally,

---

requirements (*see* Kinard v. Augusta Sash & Door Co., 336 S.E.2d 465, 467 (S.C. 1985) (stating that in "bystander" cases seeking recovery for negligent infliction of emotional distress "the plaintiff and the victim must be closely related"); restricted the types of damages that are recoverable (*see* Rieck v. Medical Protective Co., 219 N.W.2d 242, 245 (Wis. 1974) (denying recovery of child-rearing costs in failure-to-diagnose-pregnancy cases because that element of damages would be "wholly out of proportion to the culpability involved"); embraced comparative responsibility defenses (RESTATEMENT, THIRD, OF TORTS: LIABILITY FOR PHYSICAL HARM (BASIC PRINCIPLES) § 25 (Proposed Final Draft No. 1, 2005) (discussing the defense in strict-liability cases); and limited recovery of damages to harm proximately caused (*see* RESTATEMENT, THIRD, OF TORTS: LIABILITY FOR PHYSICAL HARM (BASIC PRINCIPLES) Ch. 6 (Proposed Final Draft No. 1, 2005) (discussing scope of liability).

[273] *Cf.* People v. Ware, 2003 W.L. 22120898, *2 (Cal. Ct. App.) (affirming an award against the perpetrator of restitutionary damages, including an amount for value of business hours spent by the victim on repairing her damaged credit, because the legislature intended "that a victim of crime who incurs any economic loss as a result of the commission of a crime shall receive restitution directly from any defendant convicted of that crime").

[274] "In the absence of physical damage, tort recovery for pure economic loss is limited to 'wilful' infliction of economic loss." O'Brien, *supra* note 243, at 959-60.

[275] See note 177, *supra*, and the accompanying text.

[276] *See* JAY M. FEINMAN, ECONOMIC NEGLIGENCE, *supra* footnote 245, at 11 (1995) (stating that "[t]he traditional view is that personal injury is qualitatively different from economic loss because the former often has catastrophic consequences for the victim and because monetary compensation is unable to wholly remedy injury of this kind; therefore, negligence principles should be confined to cases of personal injury. This view is now controversial; it has been challenged by many courts. .. ."); CRITICAL INFORMATION INFRASTRUCTURE, *supra* note 12, at 50 (opining that "[m]any courts . . . are beginning to reject the economic loss doctrine. For example, in People Express Airline v. Consolidated Rail Corporation [495 A.2d 107 (N.J. 1985)], the New Jersey Supreme Court concluded that 'a defendant who has breached his duty of care to avoid the risk of economic injury to particularly foreseeable plaintiffs may be held liable for actual economic losses that are proximately caused by its breach of duty'").

virtually all states that embrace the economic-loss rule recognize some exceptions.[277] For example, economic damages are routinely recoverable in negligent misrepresentation actions.[278] Many states also allow persons whose legacies are lost due to negligent preparation of a will to sue to recover those economic damages.[279] A court might determine the relationship between a database possessor and data subject is sufficiently "special"[280] to warrant recovery of out-of-pocket losses resulting from identity theft–notwithstanding the economic-loss rule.

B. Emotional-Distress Damages

States differ tremendously in what they say about whether negligently caused emotional distress is actionable.[281] Some jurisdictions hold that such damages may almost never be recovered,[282] while others seem quite willing to entertain claims for psychic suffering caused by failure to exercise care.

One arena in which a consensus of sorts has emerged are the fear-of-disease cases.[283] In these suits, the plaintiff alleges that, as a result of the defendant's tortious conduct, he or she was subjected to emotional distress based on fear of contracting a contagious disease. Many of the cases have involved fear of contracting HIV or AIDS, but the precedent extends somewhat further to fear of cancer and other diseases.

In addressing these claims, courts generally hold that a plaintiff may only recover

---

[277] *See, e.g.*, Laubmeier, *supra* note footnote 242, at 235-43 (discussing exceptions in Wisconsin).

[278] *See* RESTATEMENT, SECOND, OF TORTS § 552B (1977) (allowing recovery of out-of-pocket losses resulting from negligent misrepresentation).

[279] *See, e.g.*, Heyer v. Flaig, 449 P.2d 161, 163 (Cal. 1969) (stating that "[a]n attorney who negligently fails to fulfill a client's testamentary directions incurs liability in tort for violating a duty of care owed directly to the intended beneficiaries").

[280] J'Aire Corp. v. Gregory, 157 Cal. Rptr. 407, 410 (Cal. 1979) (stating that "[w]here a special relationship exists between the parties, a plaintiff may recover for loss of expected economic advantage through the negligent performance of a contract although the parties were not in contractual privity").

[281] *See* JOHNSON & GUNN, *supra* note 33, at 577 (noting that "[n]o area of tort law is more unsettled than compensation for negligent infliction of emotional distress. The decisions continually restate the criteria for recovery, and there are often substantial differences in the requirements, or their interpretation, from one jurisdiction to the next, and within any one jurisdiction at different times").

[282] *Cf.* Charles E. Cantu, *An Essay on the Tort of Negligent Infliction of Emotional Distress in Texas: Stop Saying It Does Not Exist*, 33 ST. MARY'S L.J. 455, 465 (2002) (discussing the Texas Supreme Court's retreat from a broad interpretation of the tort).

[283] *See generally* Kimberly Simmons, *Recovery for Emotional Distress Based on Fear of Contracting HIV or AIDS*, 59 A.L.R. 5th 535, § 2(a) (Westlaw 2005) (stating that "[m]ost often crucial to the success of a claim is whether the particular jurisdiction or court required proof of actual exposure to a disease-causing agent").

emotional distress damages if the plaintiff was actually "exposed" to the disease.[284] Fear of disease in the absence of exposure is deemed to be unreasonable and therefore not compensable.[285]

"Of course the critical question is whether 'exposed' means (a) that the defendant had the disease [when he or she came into contact with the plaintiff], (b) that the circumstances were such that the disease might have been transmitted, © that it is probable that the plaintiff will develop the disease, or (d) that the plaintiff in fact contracted the disease."[286] Courts have differed in answering this question,[287] yet the precedent that has emerged in these cases provides a logical starting point for determining whether a data subject should be able to recover for emotional-distress losses resulting from unauthorized database intrusion and fear of identity theft or other harm. If there is no evidence that the plaintiff's data was actually accessed by an intruder, but only a risk of unauthorized access, emotional distress damages, which are inherently difficult to quantify, ordinarily should be denied. For example, in some cases the evidence shows that "hackers appeared to have been more interested in using . . . [a university's] computer to download movies and music than to access personal data."[288]

In proving that the plaintiff's personal data were subject to unauthorized access, it may be appropriate for courts to employ a presumption of unauthorized access. If the defendant has allowed or caused the best evidence of exposure to be lost or destroyed, it may be reasonable to

---

[284] *See* Majca v. Beekil, 701 N.E.2d 1084 (Ill. 1998) (holding that a complaint which alleged that a dental student was infected with HIV at time he provided treatment failed to state a cause of action for fear of contracting AIDS, absent an allegation that the patients were actually exposed to HIV); K.A.C. v. Benson, 527 N.W.2d 553 (Minn. 1995) (holding that a patient who did not allege that she was actually exposed to HIV was not in the zone of danger and could not recover for negligent infliction of emotional distress). *See also* Brzoska v. Olson, 668 A.2d 1355 (Del. 1995) (holding that damages for emotional distress are recoverable only if underlying physical injury is shown). *But see* Temple-Inland Forest Products Corp. v. Carter, 993 S.W.2d 88 (Tex. 1999) (holding that workers who were exposed to asbestos, but who did not then have an asbestos-related disease, could not recover damages for fear of developing such a disease in the future).

[285] *But see* Madrid v. Lincoln County Med. Ctr., 923 P.2d 1154, 1159 (N.M. 1996) (permitting recovery without exposure where the plaintiff was negligently allowed to come into contact with bodily fluids that might have been, but were not, HIV-positive).

[286] JOHNSON & GUNN, *supra* note 33, at 579.

[287] *Compare* Johnson v. West Va. Univ. Hosp., 413 S.E.2d 889, 893 (W. Va. 1991) (permitting recovery where the defendant hospital negligently failed to advise a security officer that an unruly patient had AIDS, and the patient bit the officer after biting himself), *with* Potter v. Firestone Tire & Rubber Co., 863 P.2d 795, 800 (Cal. 1993) (holding that damages for fear of cancer in a negligence action are allowed only if the fear stems from a knowledge which is corroborated by reasonable medical and scientific opinion that it is more likely than not that cancer will develop in the future due to the toxic exposure).

[288] Ensslin, *supra* note 9 (explaining that the hackers had access to information about 42,900 persons).

assume that exposure occurred, absent proof to the contrary. There are fear-of-disease cases that take this approach.[289]

In cases involving *intentional* infliction of emotional distress, courts have been assiduous in requiring that the distress be severe before it is compensable.[290] This severity requirement is all the more applicable to cases where distress is based upon mere alleged negligence. Presumably this means that only in rare cases will it be possible for a data subject who does not suffer physical harm to recover emotional distress damages relating to data intrusion.

C. Security-Monitoring Damages

Database possessors whose security has been breached are often reluctant to discover and report such developments[291] for fear of triggering adverse publicity, legal liability,[292] or increased attacks by hackers.[293] As a result, there is often an undesirable lag between the occurrence of an intrusion, discovery of that breach, and revelation of the events to data subjects.[294] Indeed, sometimes data subjects are never told.[295] Yet, as noted above,[296] revelation that a breach of security has occurred enables data subjects to protect their interests through increased vigilance

---

[289] *See* South Cent. Reg. Med. Ctr. v. Pickering, 749 So. 2d 95 (Miss. 1999), (holding that if the defendant has allowed or caused the best evidence of exposure to HIV or another communicable disease to be destroyed, despite the fact that defendant had notice that an issue existed regarding that evidence, a rebuttable presumption of actual exposure arises in favor of the plaintiff).

[290] *See, e.g.*, Russo v. White, 400 S.E.2d 160, 163 (Va. 1991) (allowing recovery only where "distress is so severe that no reasonable person could be expected to endure it")

[291] *See* Preston & Turner, *supra* note 22, at 459-60 (stating that "[u]nderreporting computer security incidents is not limited to the U.S.–one European study estimates 30,000 to 40,000 occurred in one European nation, while only 105 official complaints were made"); Wibel, *supra* note 12, at 1612 n.170 (stating that reluctance to report security vulnerability in part reflects "a lack of faith in law enforcement").

[292] *See* Marc S. Friedman & Kristin Bissinger, *Infojacking: Crimes on the Information Superhighway*, 9 NO. 5 J. PROPRIETARY RTS. 2, 2 (1997) (stating that "organizations often swallow losses quietly rather than notifying the authorities and advertising their vulnerability to shareholders and clients").

[293] *See* CRITICAL INFORMATION INFRASTRUCTURE, *supra* note 12, at 35 (stating that "information in the public domain about the vulnerability of a network could lead to copycat attacks"); Wibel, *supra* note 12, at 1578 n.6 (asserting that some companies fear that disclosure "both invites retributive attacks and highlights vulnerabilities to other hackers").

[294] *See* Calif. Bill Analysis, Senate Floor, 2001-2002 Regular Session, Assembly Bill 700, Aug. 22, 2002, *available in* Westlaw at CA B. An., A.B. 700 Sen., 8/22/2002 (discussing hearings "to explore why . . . [a] breach, which reportedly occurred on April 5, 2002, was not discovered until May 7, 2002 and employees were not notified until May 21, 2002").

[295] *See id.* (discussing a case where "a former employee sold hundreds of financial records to an identity theft ring but the company never told its customers").

[296] See note 204, *supra*, and the accompanying text.

against identity theft and other types of harm.[297]

Notification can also be consistent with a database possessor's own interests. Timely notice to customers may protect a company's reputation, reduce its risk of legal liability, and minimize the chances of customer defections. [298] "Requiring businesses to disclose information security violations [also] provides operators with a market incentive to ensure that their security is adequate."[299]

State security breach notification laws currently provide only a limited incentive for database possessors to discover intrusion, because notification obligations are ordinarily based not upon when the breach should have been discovered, but on actual discovery or notification of the intrusion.[300] In addition, the civil fines that apply to a breach of a general statutory duty to protect customer information are typically capped at a low amount, which may provide insufficient inducement for best practices.[301]

Because "[v]ictims of identity theft must act quickly to minimize . . . damage . . . [and] expeditious notification of possible misuse of a person's personal information is imperative,"[302] database possessors should be given a legal incentive to discover and report unauthorized database intrusions. That incentive could take the form of a limitation on liability. One reasonable option would be to cap the database possessor's exposure to liability at the moment that the breach is revealed to the data subject.[303] Notification could serve as the pivotal factor in shifting further responsibility (beyond the damages cap) from the data possessor to the data subject. Once notice of the security breach is provided, the data subject is in a better position than the defendant to monitor the risk of harm and to take action against threats to his or her

---

[297] *See* CRITICAL INFORMATION INFRASTRUCTURE, *supra* note 12, at 59 (stating that "[d]isclosure is a common vehicle for consumer protection"); Preston & Turner, *supra* note 22, at 460 (stating that "when consumers have notice of unauthorized access to their personal information, they can take steps to mitigate the potential harm by informing credit reporting agencies and responding to fraudulent attempts to exploit their good names").

[298] Interagency Guidance, *supra* note 215.

[299] Preston & Turner, *supra* note 22, at 460.

[300] *See, e.g.*, LA. REV. STAT. § 51:3074(A), La. Legis. 499 (2005) ("shall, following discovery of a breach . . . , notify"); TEX. BUS. & COM. CODE § 48.103, Tx. Legis. 294 (2005) (providing that businesses "shall disclose . . . after discovering or receiving notification of the breach").

[301] *See, e.g.*, TEX. BUS. & COM. CODE § 48.201(a), Tx. Legis. 294 (2005) stating that "[a] person who violates this chapter is liable to the state for a civil penalty of at least $2,000 but not more than $50,000 for each violation"); *id.* at § 48.201(e) (allowing recovery of "reasonable expenses . . . including reasonable attorney's fees, court costs, and investigatory costs").

[302] LA. REV. STAT. § 51:3072, La. Legis. 499 (2005) (legislative finding).

[303] The database possessor should have the duty of proving that the data subject was notified of the breach or that the possessor did everything reasonable to achieve that result. This is especially true where aggregate forms of communication are used to disclose security breaches to a large class of persons.

credit and personal security.

The cap on damages could take the form of limiting liability to an amount equivalent to the out-of-pocket costs of monitoring security and taking reasonably necessary steps to prevent identity theft and other losses. These "security monitoring damages" would be similar in concept to the medical monitoring damages which some state[304] and federal[305] courts allow victims of toxic exposure to recover. The analogy is apt, as at least one court has found.[306] A

---

[304] *See, e.g.,* Potter v. Firestone Tire and Rubber Co., 863 P.2d 795, 824-25 (Cal. 1993) (stating that "the cost of medical monitoring is a compensable item of damages where . . . the need for future monitoring is a reasonably certain consequence of a plaintiff's toxic exposure and that the recommended monitoring is reasonable. In determining the reasonableness and necessity of monitoring, the following factors are relevant: (1) the significance and extent of the plaintiff's exposure to chemicals; (2) the toxicity of the chemicals; (3) the relative increase in the chance of onset of disease in the exposed plaintiff as a result of the exposure, when compared to (a) the plaintiff's chances of developing the disease had he or she not been exposed, and (b) the chances of the members of the public at large of developing the disease; (4) the seriousness of the disease for which the plaintiff is at risk; and (5) the clinical value of early detection and diagnosis"); Askey v. Occidental Chemical Corp., 477 N.Y.S.2d 242, 247 (App. Div. 1984) (allowing recovery of medical monitoring damages to "permit the early detection and treatment of maladies" and holding that "as a matter of public policy the tort-feasor should bear its cost"); Redland Soccer Club, Inc. v. Dep't of the Army, 696 A.2d 137, 145 (Pa. 1997) (finding "no reason to limit common law medical monitoring claims to asbestos-related injuries"); Bower v. Westinghouse Elec. Corp., 522 S.E.2d 424, 429 (W. Va. 1999) (recognizing a cause of action). *But see* Henry v. Dow Chemical Co., 2005 W.L. 1869555, *4 (Mich.) (holding that medical monitoring was not a cognizable negligence claim absent physical injury); Badillo v. American Brands, Inc., 16 P.3d 435, 441 (Nev. 2001) (holding that "Nevada common law does not recognize a cause of action for medical monitoring" and that while a "remedy of medical monitoring may be available for an underlying cause of action . . . neither party . . . briefed the issue nor set forth the cause of action to which it would provide a remedy").

Absent direct exposure to a toxic substance, medical-monitoring damages may be denied. *See, e.g.*, Theer v. Philip Carey Co., 628 A.2d 724 (N.J. 1993) (holding that an asbestos worker's wife, who was exposed to product only in an indirect manner, was not entitled to recover medical surveillance damages in a products liability action against manufacturers of asbestos products).

[305] *See, e.g.*, Carey v. Kerr-McGee Chem. Corp., 999 F. Supp. 1109 (N.D. Ill.1998) (predicting Illinois law); *Witherspoon v. Philip Morris, Inc.,* 964 F. Supp. 455, 467 (D.D.C.1997) (recognizing medical monitoring damages under District of Columbia law, but finding that the plaintiff failed to prove "present injury and a reasonable fear that the present injury could lead to the future occurrence of disease").

[306] *See* Stollenwerk v. TriWest Health Care Alliance, No. 03-0185 PHX SRB (D. Ariz.), *discussed at* eplaw.us/news/2005/05/20 (last visited Aug. 9, 2005) (finding that awarding monitoring fees would promote early detection of identity theft). *See also* People v. Ware, 2003 W.L. 22120898, *2 (Cal. Ct. App.) (affirming an award of restitutionary damages against the perpetrator of identity theft which included "$100 per year for monitoring the adverse

data subject whose personal data has been exposed to a breach of security, like a person who suffers exposure to a toxic substance, is at risk of further harm. There is no certainty that the harm (e.g., identity theft in the case of the data subject or perhaps cancer in the case of the toxic-exposure victim) will ever occur. The reasonable and prudent course in light of those risks is to incur the expenses that are necessary to monitor the risk that harm may develop. The victim of the exposure is thereby placed in a position to take prompt action–in one case, to combat the risk of financial harm and other risks from data misuse, and in the other, to secure necessary medical care to address a developing illness or condition.

The concept of shifting responsibility is not new to the law.[307] There are cases which hold that there are sometimes good reasons for a court to hold that a party who created a risk is not a proximate cause of harm that later occurs.[308] In these cases, the responsibility for preventing the harm has shifted from the original tortfeasor to someone else. While the law has typically shied away from the rubric of "shifting responsibility," there are many instances where tort law has embraced the idea in substance, sometimes dressed in the garb of "duty." The rules, mentioned earlier, which say that a possessor of land need do nothing more than warn a licensee of known dangers,[309] or that in some states a mental health professional treating a dangerous

---

consequences on her credit rating").

[307] *See generally* RESTATEMENT, SECOND, OF TORTS § 452 cmt. f (1965) (discussing the shifting of responsibility to a third person).

[308] In some cases, a contractual or statutory allocation of responsibilities between multiple parties is important. *See* Goar v. Village of Stephen, 196 N.W. 171 (Minn. 1923) (holding that the duty to prevent harm had shifted from a power company that negligently installed electrical lines to a village, which had contractually assumed the obligation of inspecting the lines); First Assembly of God v. Texas Utilities, 52 S.W.3d 482, 492 (Tex. App. 2001) (holding that where a statutory tariff which provided that "the Customer assumes full responsibility for electric energy at the point of delivery," a utility did not have a duty to check equipment "downstream' to insure that it was installed and maintained properly). In other cases, the determination is a result of a number of factors, such as the degree of danger and the magnitude of the risk of harm; the character and position of a third person and his or her relationship to the plaintiff or defendant; the actors' knowledge of the danger; the likelihood that someone other than the antecedent tortfeasor would exercise care; amount of time that elapsed since the original negligence. *See* RESTATEMENT, SECOND, OF TORTS § 452 cmt. f (1965) (discussing factors). In some cases, the courts seem to implicitly ask whether the defendant did everything reasonable to prevent the harm from occurring. *See, e.g.*, Balido v. Improved Machinery, Inc., 105 Cal. Rptr. 890 (App. Ct. 1973) (holding that the responsibility to prevent a defective machine from causing harm did not shift from the manufacturer, who offered to repair the machine for $500, to the subsequent party who refused the offer). *See also* Kent v. Commonwealth, 771 N.E.2d 770 (Mass. 2002) (holding that a board's decision to parole an inmate pursuant to an INS deportation warrant shifted the duty to prevent harm to the INS); Braun v. New Hope Twp., 646 N.W.2d 737 (S.D. 2002) (holding that the responsibility to prevent a motorist's injuries shifted from farmers who broke a warning sign to a township that had a duty to erect and maintain warning signs).

[309] *See* footnote 212, *supra*.

patient need only warn the victim or the police,[310] are rules that, in effect, shift the burden of preventing harm from one party to another once a warning is given.

The bargain of capping a cybersecurity plaintiff's damages at the cost of monitoring security if the database possessor provides notification of a security breach is not a bad one. From the standpoint of the data subject, the plaintiff may be better off with a warning and reimbursement for the out-of-pocket costs of vigilance, than with gambling on a tort action against the database possessor. That suit would be fraught with many obstacles: a possibly short statute of limitations,[311] if the improperly accessed data is not exploited by the intruder promptly; a risk that the database possessor's negligence might not be found to be a proximate cause of resulting criminal conduct;[312] the likelihood that the economic-loss or "exposure" rules may bar important aspects of damages;[313] and the possibility that the court might find that the possessor had no duty at all.

The bargain is also not bad for database possessors. Capping damages at the cost of security-monitoring damages would avoid the risk of catastrophic liability for personal injuries that sometimes occur; exposure to property-damage claims; and the chance that a court might narrowly construe the applicability of the economic-loss rule. Some companies faced with the risk of liability from loss of personal data have voluntarily chosen to provide affected persons with a type of security-monitoring protection.[314]

Moreover, society would be better off if damages were capped at the cost of security monitoring in exchange for notification whenever security is breached. The only way to minimize the losses related to database intrusions (aside from criminal penalties, which seem not

---

[310] *See* footnote 213, *supra*.

[311] The federal government says that victims of data intrusion should "remain vigilant over the next twelve to twenty-four months." Interagency Guidance, *supra* note 215. In some states, the applicable statute of limitations for negligence might be two years, depending on the nature of the claim. *See* TEX. CIV. PRAC. & REM. CODE § 16.003(a) & (b) (Westlaw current through Ch. 290 of the 2005 Reg. Sess. 79th Legislature) (stating that a two-year statute applies to certain claims for personal injury, property damage, and wrongful death).

[312] *See generally* RESTATEMENT, SECOND, OF TORTS § 448 (1965) (discussing whether intentionally tortious or criminal conduct breaks the chain of causation).

[313] See Parts IV-A and B, *supra*.

[314] *See* Dash, *supra* note 10 (discussing a television spot highlighting "Citigroup's free identity theft protection services, which include fraud detection warnings on every bank and credit card account"); McCoy, *supra* note 38, at 490-91 (stating that, upon learning of the theft of laptops containing customer information in November 2003, Wells Fargo notified the affected customers and promised to monitor the at-risk accounts, change the affected account numbers, add a Credit Alert report to customers' credit reports, provide 24-hour access to specially trained account representatives, and provide a one-year membership to a credit-monitoring reporting service so customers could quickly learn if any of their information was being misused"). *See also* Reddick, *supra* note 11, at 1 (noting that nine states require businesses to notify consumer-reporting agencies of security breaches)

very effective) is to spur investment in data security, discover when intrusions occur, and warn persons whose interests are at risk. A cap on damages in exchange for notification of security breaches would not undercut the incentives database possessors have to invest in data security. Companies and others would still be subject to state and federal laws which impose various sanctions relating to cybersecurity; they would still face the threats of bad publicity and consumer disaffection resulting from disclosure of security breaches; and at least some possessors (e.g., credit card companies) would still stand to lose millions of dollars as a result of fraudulent use of personal information. However, the damages cap in the form of liability only for security-monitoring damages would help to ensure that database possessors are not subject to ruinous tort judgments. It would create an incentive to discover security breaches and to internalize the security monitoring costs that those intrusions entail. Consumers would also be better able to protect their own interest in the variety of ways discussed above. In addition, the cap on damages might also reduce the threat of overburdening already overworked federal and state courts. The damages issues in cybersecurity cases would be greatly simplified, and it is likely that guidance from the courts would quickly define the average costs of security monitoring, thereby promoting the settlement of cases. Indeed, limiting liability to security-monitoring damages is also likely to promote the growth of insurance to cover intruder-related losses by making the extent of liability more certain and thereby facilitating the pricing of insurance coverage.[315]

A damages cap should not apply to cases involving egregious conduct. A plaintiff who can establish that the defendant acted with reckless indifference or intentional disregard in failing to protect data should be able to avoid the limitation on liability. Similarly, if no disclosure of a security breach is made, liability for a breach of that duty or of the duty to protect data should extend as far as the usual rules of tort law allow.

A cap on database possessor liability at the costs of security-monitoring damages could be legislatively enacted.[316] However, in the absence of legislation to the contrary, questions relating to duty, proximate causation (including shifting responsibility), and damages have been the traditional province of the courts. Quite possibly it would be permissible under state law, for the courts to determine that if a database possessor negligently fails to protect computerized personal information, there is no legal obligation other than to pay for security monitoring damages, if the breach is revealed to the data subject.

---

[315] *See* CRITICAL INFORMATION INFRASTRUCTURE, *supra* note 12, at 65-66 (describing available coverage and noting that the "paucity of data on cyberrelated losses makes it difficult to accurately price cyberinsurance policies").

[316] *See* Victor E. Schwartz, Mark A. Behrens, Emma K. Burton, & Jennifer L. Groninger, *Medical Monitoring: Should Tort Law Say Yes?*, 34 WAKE FOREST L. REV. 1057 (1999) (stating that "the inherent complexities and significant public policy concerns surrounding medical monitoring awards, which were noted by the United States Supreme Court in Metro-North [521 U. S. 424 (1997)], suggest that the issue ought to be decided by legislatures, not by courts").

V. Conclusion: Security in Insecure Times

Modern society is built on fragile foundations of computerized personal data. If this society is to endure and prosper, then those foundations must be vigilantly safeguarded. Tort law offers an appropriate legal regime for allocating the risks and spreading the costs of database intrusion-related losses. Tort law can also be employed to create incentives, on the part of both data possessors and data subjects, to minimize the losses associated with breaches of database security. Courts and legislatures must consider carefully the role of tort liability in protecting the computerized foundations of modern society. If those who make and interpret the laws are too hasty in concluding that database possessors are not liable for losses occasioned by unauthorized data access–whether because there is no duty, no proximate causation, or no recoverable damages–important opportunities to reduce and distribute the costs of computerized technology will be lost. If liability is too readily assessed, important institutions will be adversely affected, and with them the prosperity of modern society. Security in insecure times requires a sensitive balancing of competing interests. Established tort principles carefully applied to the contemporary problems of cybersecurity and identity theft can perform a key role in protecting the economic foundations of modern life.