Texas Wesleyan Law Review

Volume 18 | Issue 2 Article 3

12-1-2011

Hacking, Theft, and Corporate Negligence: Making the Case for Mandatory Encryption of Personal Information

Stephen J. Rancourt

HACKING, THEFT, AND CORPORATE NEGLIGENCE: MAKING THE CASE FOR MANDATORY ENCRYPTION OF PERSONAL INFORMATION

By: Stephen J. Rancourt†

ABSTRACT

Information is being created at an astonishing rate, and the electronic storage of personal data is at the forefront of this growth. Social security numbers, home and email addresses, and financial records are almost universally stored electronically, whether on internal servers, hard drives, or portable devices, such as flash drives and diskettes. The ubiquity of this information has undoubtedly benefitted commerce, but it has not come without drawbacks. As recent evidence suggests, personal information is increasingly vulnerable to hacking and other forms of theft, putting the consumer at serious risk of identity theft and misuse of their personal information. The time has come for a uniform standard to protect this type of data, as well as statutory liability for companies that fail to store this information properly. This Article attempts to show why current statutory and common law is inadequate to solve this problem and makes the case for creating a national standard of encryption for businesses that store personal information.

TABLE OF CONTENTS

† J.D., *cum laude*, University of Richmond School of Law. I would like to thank Professor James Gibson, who provided me with tremendous guidance throughout the editing and publication process, as well as my wife, Whitney, whose love and patience with me makes all things possible.

DOI: https://doi.org/10.37419/TWLR.V18.I2.2

I. INTRODUCTION

The amount of electronic data generated in recent years has increased exponentially. In 2002, the amount of data stored on computers worldwide was around 5 exabytes, equivalent to 5 billion gigabytes.[1] By 2009, that number had increased to around 988 exabytes,[2] almost 200 times the total amount of data that existed only seven years previously. If all this information were printed and stacked, the pile would extend all the way to Pluto and back.[3]

Some of this data is inherently personal. Completing a transaction online requires providing credit card information, which is then stored by that online retailer for billing or for future purchases. Banking and investing is increasingly done over the Internet, and today, a person's entire investment portfolio, including bank account numbers, stocks, and retirement accounts could be kept on the servers of a single investment clearinghouse. An employee's personal information, including home address, phone, and Social Security number is routinely kept on a company database and saved on the firm server or even a manager's laptop. Even something as basic as your email address is stored in dozens of places online—think about the last time you subscribed to a free online newspaper or applied to an online job posting.

As the volume of this type of data has increased, so have the instances of hacking and computer theft that result in personal information being exposed. In 2008, the inadequate security measures at online pharmacy Express Scripts, Inc. allowed unauthorized persons to gain access to the confidential information of its members.[4] These persons were able to steal the names, dates of birth, Social Security numbers, and prescription information of all Express Scripts customers, and they threatened to make the information public unless the company paid a ransom.[5] Similarly, a flaw in TD Ameritrade's online security system made it possible for hackers to steal the account information for all of the company's 6.3 million customers.[6] The hackers were able to obtain private information including customer names,

1. *See* Bennett B. Borden, *E-Discovery Alert, The Demise of Linear Review*, WILLIAMS MULLEN, 1 (Oct. 2010), *available at* http://www.clearwellsystems.com/e-discovery-blog/wp-content/uploads/2010/12/E-Discovery_10-05-2010_Linear-Review_1.pdf.

2. *Id.*

3. *See* Jason R. Baron & Ralph C. Losey, *e-Discovery: Did You Know?*, YOUTUBE (Feb. 11, 2010), http://www.youtube.com/watch?v=bWbJWcsPp1M.

4. *See* Amburgy v. Express Scripts, Inc., 671 F. Supp. 2d 1046, 1049 (E.D. Mo. 2009).

5. *See id.*

6. *See* David Kravets, *Ameritrade Hack Settlement: $2 Per Victim, $1.8 Million for Lawyers*, WIRED (July 11, 2008), http://www.wired.com/threatlevel/2008/07/ameri

phone numbers, home addresses, and email accounts, which were then used to "spam"[7] TD Ameritrade Accountholders.[8]

Well-publicized events of the past year have shown just how big this problem has become. In April, a large email marketing company called Epsilon Data Management fell victim to a massive data breach.[9] The company, which sends over 40 billion emails annually on behalf of over 2,500 clients, admitted that roughly 2% of their entire client database was hacked into and stolen.[10] Customers of companies including Ethan Allen, Lacoste, and 1-800-Flowers received emails informing them that their email addresses had been compromised and were told to be extra vigilant in avoiding "phishing"[11] schemes.[12] Only a couple weeks later, the Sony Playstation Network was hacked into, affecting over 70 million users worldwide.[13] After staying silent for a week, Sony eventually confirmed that hackers may have obtained credit card information, names, home addresses, and login passwords for an unknown number of accountholders.[14]

Other means of unlawfully obtaining others' personal information have been less technologically advanced. In October 2008, someone stole a laptop computer from a Starbucks in the state of Washington.[15] The laptop was owned by the company, and contained the unencrypted names, addresses, and Social Security numbers of 97,000 Starbucks employees.[16] One employee in particular claimed that his bank had notified him that someone had attempted to open a new

---

trade-hack/; *In re* TD Ameritrade Accountholder Litig., 266 F.R.D. 418, 419 (N.D. Cal. 2009).

7. *Spam*, TECHTERMS.COM, http://www.techterms.com/definition/spam (last visited Sept. 21, 2011) ("Originating from the name of Hormel's canned meat, 'spam' now also refers to junk e-mail or irrelevant postings to a newsgroup or bulletin board. The unsolicited e-mail messages you receive about refinancing your home, reversing aging, and losing those extra pounds are all considered to be spam.").

8. *See* Kravets, *supra* note 6; *In re TD Ameritrade*, 266 F.R.D. at 419.

9. *See* Lisa Greim, *Breached E-Mail Marketer Sends Billions of E-Mails a Year*, PCWORLD, (Apr. 5, 2011), http://www.pcworld.com/article/224373/breached_email_marketer_sends_billions_of_emails_a_year.html.

10. *Id.*

11. Phishing (pronounced "fishing") is a con game that scammers use to collect personal information from unsuspecting users. Phishers will send out emails that appear to come from legitimate websites, which will state that users' information needs to be updated or validated. The email will often provide a link to a web address which will then ask users to enter their usernames, passwords, and other confidential information. *Phishing*, TECHTERMS.COM, http://www.techterms.com/definition/phishing (last visited Sept. 21, 2011).

12. *Greim*, *supra* note 9.

13. Jason Schreier, *PlayStation Network Hack Leaves Credit Card Info at Risk*, WIRED (Apr. 26, 2011), http://www.wired.com/gamelife/2011/04/playstation-network-hacked/.

14. Mark Hachman, *Sony: PlayStation Network Hack Nabbed Personal Info, Maybe Credit Cards*, PCMAG.COM, Apr. 26, 2011, http://www.pcmag.com/article2/0,2817,2384353,00.asp.

15. Krottner v. Starbucks Corp., 628 F.3d 1139, 1140 (9th Cir. 2010).

16. *See id.*

account using this information, and this event formed the basis for a class action lawsuit against the company.[17] Loss of electronic storage devices containing sensitive personal information is now routine; the recent failure to secure a British Petroleum employee's laptop is only one of many recent examples where the personal data of thousands of innocent persons have been put in jeopardy.[18]

With identify theft, spamming, and misuse of personal information becoming of increasing concern in modern society, the question arises: What should be the extent of a company's liability for failing to protect the personal data of its customers and employees? Courts have taken differing views regarding liability for these types of transgressions, and the issue of standing has become a focal point for litigation. Plaintiffs bringing suit under common law claims have often found difficulty in proving actual damages, and federal statutes have thus far proven inadequate to spur corporate action.

The answer to the problem lies in encryption. A few states have taken the lead in encouraging companies to adhere to specific encryption standards for the electronic storage of all personal information in electronic format.[19] These statutes should form the basis for a new national standard, with congressional action needed to incentivize the proper storage and transmission of personal data. Part II will consider the previous cases brought under common law claims and the problems that plaintiffs have faced regarding Article III standing and proving damages. Part III will look at the current statutory regime and the most recent state-level legislation imposing specific encryption standards for the storage of personal information. Finally, Part IV will make the case for using these new state statutes as a basis for congressional legislation, and why the adoption of a uniform law will benefit both companies and the persons whose information they possess.

---

17. *Id.* at 1141.

18. *See, e.g.*, Jaikumar Vijayan, *BP Employee Loses Laptop Containing Data on 13,000 Oil Spill Claimants*, COMPUTERWORLD (Mar. 29, 2011), http://www.computerworld.com/s/article/9215316/BP_employee_loses_laptop_containing_data_on_13_000_oil_spill_claimants ("The personal information of 13,000 individuals who had filed compensation claims with BP after [the Deepwater Horizon] oil spill may have been compromised after a laptop containing the data was lost by a BP employee. The [unencrypted] information . . . included the names, Social Security numbers, addresses, phone numbers, and dates of birth of [all these individuals]. The lost laptop was immediately reported to law enforcement authorities and BP security, but has not been located despite a thorough search . . . .").

19. *See, e.g.*, Standards for the Protection of Personal Information of Residents of the Commonwealth, 201 MASS CODE REGS. 17.04 (2008); Security of Personal Information, NEV. REV. STAT. ANN. § 603A.215 (LexisNexis 2010).

II. Recent Case Law Involving the Failure to Properly Secure Personal Data

The explosion in data generation and storage of personal information has given rise to theft and misuse of this data. Employees and customers who find their information compromised have often found the guilty party unwilling to compensate them for their losses, leaving the courts to decide the degree and amount of liability. Recent events have spurred a tremendous amount of litigation from plaintiffs seeking damages for the loss of their personal information.[20] Class action lawsuits have thus far proven to be the preferred method of seeking redress through litigation, but with limited success. In many of these cases, meeting the requirements for Article III standing has become the major issue of contention, and many of these suits have been dismissed as a result. Should a plaintiff be able to show standing to sue, the issue then becomes one of proving damages, an issue that is often hard to win for many plaintiffs. This Section will discuss both of these issues, and show why recent suits under common-law claims have thus far proven to be an inadequate remedy.

A. *The Issue of Standing*

Under Article III, Section 2 of the United States Constitution, federal judicial power is limited to the resolution of "Cases" and "Controversies"[21] that may be appropriately resolved through the judicial process.[22] One element of this case-or-controversy obligation is that

20. *See, e.g.*, Bell v. Acxiom Corp., No. 4:06CV00485-WRW, 2006 WL 2850042, at *1 (E.D. Ark. Oct. 3, 2006); Randolph v. ING Life Ins. & Annuity Co., 486 F. Supp. 2d 1, 2 (D.D.C. 2007); Amburgy v. Express Scripts, Inc., 671 F. Supp. 2d 1046 (E.D. Mo. 2009); Giordano v. Wachovia Sec., LLC, Civil No. 06-476 (JBS), 2006 WL 2177036, at *1 (D.N.J. July 31, 2006); Key v. DSW, Inc., 454 F. Supp. 2d 684 (S.D. Ohio 2006); Pisciotta v. Old Nat'l Bancorp, 499 F.3d 629 (7th Cir. 2007); Ruiz v. Gap, Inc., 380 F. App'x 689 (9th Cir. 2010); Stollenwerk v. Tri-West Healthcare Alliance, 254 F. App'x 664 (9th Cir. 2007); Willey v. J.P. Morgan Chase N.A., No. 09 Civ. 1397(CM), 2009 WL 1938987 (S.D.N.Y. July 7, 2009); Cherny v. Emigrant Bank, 604 F. Supp. 2d 605 (S.D.N.Y. 2009); Caudle v. Towers, Perrin, Forster & Crosby, Inc., 580 F. Supp. 2d 273 (S.D.N.Y. 2008); Shafran v. Harley-Davidson, Inc., No. 07 Civ. 1365(GBD), 2008 WL 763177, at *1 (S.D.N.Y. Mar. 20, 2008); McLoughlin v. People's United Bank, Inc., No. 3:08-cv-00944(VLB), 2009 WL 2843269, at *1 (D. Conn. Aug. 31, 2009); Belle Chasse Auto. Care, Inc. v. Advanced Auto Parts, Inc., No. 08-1568, 2009 WL 799760, at *1 (E.D. La. Mar. 24, 2009); Pinero v. Jackson Hewitt Tax Serv. Inc., 594 F. Supp. 2d 710, 713–14 (E.D. La. 2009); Melancon v. La. Office of Student Fin. Assistance, 567 F. Supp. 2d 873, 874 (E.D. La. 2008); Ponder v. Pfizer, 522 F. Supp. 2d 793, 795 (M.D. La. 2007); *In re* Hannaford Bros. Co. Customer Data Sec. Breach Litig., 613 F. Supp. 2d 108, 116 (D. Me. 2009); Hendricks v. DSW Shoe Warehouse, Inc., 444 F. Supp. 2d 775 (W.D. Mich. 2006); Forbes v. Wells Fargo Bank, N.A., 420 F. Supp. 2d 1018, 1020 (D. Minn. 2006); Guin v. Brazos Higher Educ. Serv. Corp., No. 05-Civ.-668 (RSK/JSM), 2006 WL 288483, at *2 (D. Minn. Feb. 7, 2006); Kahle v. Litton Loan Serv. L.P., 486 F. Supp. 2d 705, 706 (S.D. Ohio 2007).

21. U.S. Const. art. III, § 2.

22. Whitmore v. Arkansas, 495 U.S. 149, 154–55 (1990).

plaintiffs must show that they have standing to sue.[23] Over time, the Supreme Court has devised a three-part test to determine whether a plaintiff has standing.[24]

First, the plaintiff must prove that he or she has suffered an "injury in fact," defined as "an invasion of a legally protected interest."[25] This injury-in-fact must be both (a) "concrete and particularized" and (b) "actual or imminent, not 'conjectural' or 'hypothetical.'"[26] Second, the plaintiff must prove that there is a "causal connection between the injury and the conduct complained of."[27] The Supreme Court has stated that this connection must be "'fairly . . . trace[able] to the challenged action of the defendant, and not . . . th[e] result [of] the independent action of some third party not before the court.'"[28] Finally, the test for standing requires that it must be "likely," not merely "speculative," that a favorable decision will be able to redress the injury caused to the plaintiff.[29] The burden is on the plaintiff to establish all three of these elements.[30]

Plaintiffs bringing lawsuits based on the negligent handling of their personal information have often run into the problem of establishing standing, and federal courts have taken opposing stances on the issue.[31] Courts that have dismissed these suits for lack of standing have often done so based on the plaintiff's failure to prove an injury-in-fact.[32] In *Hammond v. Bank of New York Mellon Corp.*, a metal box containing unencrypted computer back-up tapes was somehow lost from a truck while being transported from Philadelphia to Pittsburgh.[33] The truck was operated by an outside transport company hired by the bank, and the lost tapes contained the names, addresses, Social Security numbers, bank account information, shareholder account information, and other financial data of approximately 12.5 million bank customers.[34] The bank notified the affected individuals and offered them twenty-four months of credit monitoring and $25,000

23. Allison v. Aetna, Inc., No. 09-2560, 2010 WL 3719243, at *2 (E.D. Pa.) (citing Interfaith Cmty. Org. v. Honeywell Int'l, Inc., 399 F.3d 248, 254 (3d Cir. 2005)).

24. *See* Lujan v. Defenders of Wildlife, 504 U.S. 555, 560–61 (1992).

25. *Id.* at 560 (citing Allen v. Wright, 468 U.S. 737, 756 (1984)).

26. *Id.* (quoting Los Angeles v. Lyons, 461 U.S. 95, 102 (1983)).

27. *Id.*

28. *Id.* at 560–61 (quoting Simon v. E. Ky. Welfare Rights Org., 426 U.S. 26, 41–42 (1976)).

29. *Id.* at 561 (quoting *Simon*, 426 U.S. at 38, 43).

30. *Id.* (citing FW/PBS, Inc. v. Dallas, 493 U.S. 215, 231 (1990)).

31. *Compare* Amburgy v. Express Scripts, Inc., 671 F. Supp. 2d 1046, 1058 (E.D. Mo. 2009), *with* Pisciotta v. Old Nat'l Bankcorp., 499 F.3d 629, 640 (7th Cir. 2007).

32. *See, e.g.*, Hammond v. Bank of N.Y. Mellon Corp., No. 08 Civ. 6060(RMB)(RLE), 2010 WL 2643307, at *8 (S.D.N.Y. June 25, 2010); *Amburgy*, 671 F. Supp. 2d 1046, 1058 (E.D. Mo. 2009); Key v. DSW Inc., 454 F. Supp. 2d 684, 685–86 (S.D. Ohio 2006); Bell v. Acxiom Corp., No. 4:06CV00485-WRW, 2006 WL 2850042, at *2 (E.D. Ark. Oct. 3, 2006).

33. *Hammond*, 2010 WL 2643307, at *2.

34. *Id.* at *2, *4.

worth of identity theft insurance.[35] Unsatisfied with this offer, a number of bank customers filed suit for negligence, breach of implied contract, and breach of fiduciary duty, and moved the court to certify the class action complaint.[36]

The U.S. District Court for the Southern District of New York held that the plaintiffs lacked standing and dismissed the suit.[37] The court noted that, of the seven named plaintiffs, only three of them had suffered from unauthorized credit transactions after the loss of the backup tapes and that these individuals had been reimbursed by the bank for these charges.[38] The other four plaintiffs admitted that they had not suffered from identity theft or other fraud and that their injuries were mainly due to an "increased risk of harm."[39] Finding these alleged injuries to be nothing more than "hypothetical and conjectural,"[40] the court granted the defendant's motion for summary judgment and dismissed the case for lack of standing.[41]

The U.S. District Court for the Eastern District of Arkansas also dismissed a class action lawsuit on the basis of standing under different facts. In *Bell v. Acxiom Corp.*, the defendant was a data bank that stored marketing information for its corporate clients, including personal, financial, and other data on its clients' customers.[42] In order for its clients to access this information, Acxiom maintained a "file transfer protocol"[43] ("FTP") site that required a username and password.[44] One of Acxiom's clients was able to access the entire Acxiom FTP server through a hole in the security system.[45] This client then downloaded the databases of Acxiom's other clients and sold the information to another marketing company, which used the names and addresses for direct mail advertisements.[46] After the client was convicted under the Computer Fraud and Abuse Act,[47] Bell (a customer

35. *Id.* at *4.
36. *Id.* at *2–4.
37. *Id.* at *14.
38. *Id.* at *5.
39. *Id.* at *5–6.
40. *Id.* at *7.
41. *Id.* at *14.
42. Bell v. Acxiom Corp., No. 4:06CV00485-WRW, 2006 WL 2850042, at *1 (E.D. Ark. Oct. 3, 2006).
43. A file transfer protocol, or FTP, "is a common method of transferring files via the Internet from one computer to another. Some common FTP programs are 'Fetch' for the Mac, and 'WS_FTP' for Windows. Many FTP servers are 'anonymous FTP' servers which means you can log in with the user name 'anonymous' and your e-mail address as the password. Other FTP servers require a specific login in order to access the files." *FTP*, TECHTERMS.COM, http://www.techterms.com/definition/ftp (last visited Sept. 29, 2011).
44. *Bell*, 2006 WL 2850042, at *1.
45. *Id.*
46. *Id.*
47. *See* United States v. Levine, 378 F. Supp. 2d 872, 873 (E.D. Ark. 2005); *see also Bell*, 2006 WL 2850042, at *1.

of one of Acxiom's clients) brought suit against Acxiom for failing to protect its clients' data.[48]

The court dismissed the plaintiff's complaint for lack of standing.[49] Although the court noted that Ms. Bell may have suffered an increased risk of identity theft, she was unable to show anything more than speculative injuries.[50] Any assertion of a future injury must be "certainly impending to constitute injury in fact,"[51] and Ms. Bell's complaint did not provide sufficient proof of this level of harm.[52] As for any increase in marketing mailing resulting from the breach, the court adopted the views of other jurisdictions and found that the receipt of unsolicited and unwanted mail did not constitute a cognizable injury.[53]

Courts have also dismissed these types of lawsuits even where the plaintiff's injuries are more particularized. In *Amburgy v. Express Scripts, Inc.*, the plaintiff alleged that he and other members of the class had spent "considerable time and money protecting themselves" after the company's inadequate security measures lead to the theft and ransom of customers' personal information.[54] After Express Scripts had notified its members of the breach, the plaintiff contended that he and other class members had suffered injury by constantly having to monitor their bank and credit card accounts.[55]

The U.S. District Court for the Eastern District of Missouri declined to hold that these allegations constituted sufficient injury-in-fact for Article III standing, at least with respect to the negligence claim.[56] Although the plaintiff had taken affirmative steps as a result of his data being potentially compromised, he was unable to show that the potential theft of his identify was imminent.[57] As the court stated:

> For plaintiff to suffer the injury and harm he alleges here, many "ifs" would have to come to pass. Assuming plaintiff's allegation of security breach to be true, plaintiff alleges that he would be injured "if" his personal information was compromised, and "if" such information was obtained by an unauthorized third party, and "if" his identity was stolen as a result, and "if" the use of his stolen identity caused him harm. These multiple "ifs" squarely place plaintiff's claimed injury in the realm of the hypothetical. If a party were al-

48. *Bell*, 2006 WL 2850042, at *1.
49. *Id.* at *2.
50. *Id.*
51. *Id.* (quoting Sierra Club v. Robertson, 28 F.3d 753, 758 (8th Cir. 1998)).
52. *Id.*
53. *See Bell*, 2006 WL 2850042, at *2 (citing Smith v. Chase Manhattan Bank, 293 A.D.2d 598, 599–600 (N.Y. App. Div. 2002); Shibley v. Time, Inc., 341 N.E.2d 337, 339–40 (Ohio Ct. App. 1975); Lamont v. Comm'r of Motor Vehicles, 269 F. Supp. 880, 883 (S.D.N.Y. 1967).
54. Amburgy v. Express Scripts, Inc., 671 F. Supp. 2d 1049, 1049 (E.D. Mo. 2009).
55. *Id.*
56. *Id.* at 1053.
57. *Id.* at 1051–52.

> lowed to assert such remote and speculative claims to obtain federal court jurisdiction, the Supreme Court's standing doctrine would be meaningless.[58]

In the court's mind, plaintiff's asserted claim of increased risk of harm was merely "conjectural or hypothetical," and therefore failed to meet the constitutional requirement for standing.[59]

A federal court in Ohio took a similar stance as the *Amburgy* court when considering the inconvenience costs associated with theft of personal information. In *Key v. DSW Inc.*, a shoe retailer collected and maintained the personal financial information of 1.5 million customers during a five-month period between 2004 and 2005.[60] As a result of improper electronic storage of this data, unauthorized persons were able to acquire the information on 96,000 of these customers, including their credit card, debit card, and checking account information.[61] In the resulting class-action lawsuit, the class members alleged that they had suffered injury-in-fact as a result of having to close their financial accounts, obtain credit reports, and purchase credit or identity-monitoring subscriptions.[62]

The court held that the increased risk of identity theft and other financial crimes was not enough to invoke Article III standing, even though many class members had taken affirmative and costly steps to prevent misuse of this data.[63] A plaintiff alleging future injury at some indefinite time simply did not meet the requirement under the first prong of the test of being an "actual or imminent" injury.[64] Citing a number of other financial theft cases dismissed for lack of standing, the *Key* court was unwilling to follow a different path, and the suit was dismissed.[65] Two years later, the Court of Appeals for the Sixth Circuit adopted this line of reasoning.[66] In dicta, and under a different set of circumstances,[67] the court agreed that the future possibility

58. *Id.* at 1053.

59. *See id.* (quoting Lujan v. Defenders of Wildlife, 504 U.S. 555, 560 (1992)); *see also* Los Angeles v. Lyons, 461 U.S. 95, 102 (1983).

60. Key v. DSW, Inc., 454 F. Supp. 2d 684, 685 (S.D. Ohio 2006).

61. *See id.* at 685–86.

62. *Id.* at 686.

63. *Id.* at 688–89.

64. *Id.* at 687, 689 (citing Lujan v. Defenders of Wildlife, 504 U.S. 555 (1992)).

65. *Key*, 454 F. Supp. 2d at 691.

66. *See* Lambert v. Hartman, 517 F.3d 433, 437 (6th Cir. 2008).

67. In *Lambert*, the plaintiff received a traffic citation for speeding, and the issuing officer filled out an Ohio Uniform Traffic Ticket containing her name, signature, home address, birth date, driver's license number, and Social Security number. *Id.* at 435. One copy of this ticket was filed in the Hamilton County Clerk's Office. *Id.* After being contacted by two retail stores concerning suspicious purchases, Ms. Lambert discovered that the Clerk's publically accessible website made it possible to search for and locate traffic citations with all this information left unredacted. *Id.* at 435–36. When she contacted the Clerk's office, they refused to remove the information, and Ms. Lambert subsequently filed suit against the county. *Id.* at 436.

of identity theft was not enough to meet the injury-in-fact requirement to successfully bring suit.[68]

This trend limiting plaintiffs' right to sue for third party data theft is beginning to shift somewhat, with some courts willing to confer Article III standing. The Seventh Circuit Court of Appeals was the first circuit to find that a threat of future harm caused by the loss or theft of personal information was enough to sufficiently show that an injury-in-fact had occurred.[69] In *Pisciotta v. Old Nat'l Bancorp*, the defendant had solicited personal information from the plaintiffs, who had applied for banking services.[70] The online forms required applicants to reveal their names, addresses, Social Security numbers, driver's license numbers, dates of birth, mother's maiden names, and any credit card or other financial account numbers.[71] The bank's website was maintained by another company.[72] Third-party hackers were able to access this information and steal the confidential information of tens of thousands of bank users and applicants.[73] When the bank sent written notice to its customers notifying them of the breach, a class action lawsuit was filed in the Southern District of Indiana.[74] The district court granted the defendant's motion for judgment on the pleadings and denied the plaintiffs' motion for class certification, holding that the plaintiffs' allegations of suffering from "substantial *potential* economic damages" did not state a cognizable injury.[75]

Although the Seventh Circuit ultimately affirmed the district court's judgment on other grounds, it disagreed with the lower court with respect to the injury-in-fact requirement, finding that the plaintiffs did have standing to sue.[76] The court analogized the harm in *Pisciotta* to cases where other circuits had found standing solely based on an increased future risk of harm, including cases involving defective medical devices, environmental pollution, and exposure to toxic chemicals.[77] The court also relied on some of its own precedent re-

68. *See id.* at 437.

69. *See* Pisciotta v. Old Nat'l Bancorp, 499 F.3d 629, 634 (7th Cir. 2007).

70. *Id.* at 631.

71. *Id.*

72. *Id.* at 632.

73. *Id.* at 631. Although the pleadings describing the exact manner of access were filed under seal, the court noted that "the scope and manner of access suggests that the intrusion was sophisticated, intentional, and malicious." *Id.* at 632.

74. *Id.* at 632.

75. *Id.*

76. *Id.* at 634, 640.

77. *See id.* at 634 n.3 (citing Denney v. Deutsche Bank AG, 443 F.3d 253, 264–65 (2d Cir. 2006) (stating in dicta that exposure to toxic substances creates a cognizable injury for standing purposes); Sutton v. St. Jude Med. S.C., Inc., 419 F.3d 568, 574–75 (6th Cir. 2005) (holding that a defective medical implement presenting an increased risk of future health problems was sufficient to confer standing); Cent. Delta Water Agency v. United States, 306 F.3d 938, 947–48 (9th Cir. 2002) (holding that "the possibility of future injury may be sufficient to confer standing on plaintiffs"); Friends of

garding future-yet-uncertain harm,[78] and ultimately concluded that "[o]nce the plaintiffs' allegations establish at least this level of injury, the fact that the plaintiffs anticipate that some greater potential harm might follow the defendant's act does not affect the standing inquiry."[79]

Relying heavily on *Pisciotta*, the Ninth Circuit has also held that the increased risk of future identity theft sufficiently established an injury-in-fact for Article III purposes.[80] In *Krottner v. Starbucks*, the names, addresses, and Social Security numbers of approximately 97,000 Starbucks employees were compromised after a laptop was stolen from one of the company's many coffee shops.[81] Although the company offered free enrollment in a credit watch service to any affected employee, a class action lawsuit alleging negligence and breach of implied contract was ultimately filed.[82]

The Ninth Circuit affirmed the district court's decision to dismiss the case for lack of standing.[83] Relying on the Seventh Circuit's analysis in *Pisciotta*, including its analogies to case law in other circuits involving medical monitoring, toxic substances, and environmental claims, the court held that the injury-in-fact requirement can satisfy Article III when the alleged act by the defendant harms the plaintiffs only by increasing their risk of future harm.[84] The court also quoted from precedent within its own jurisdiction, noting:

> [A] plaintiff may allege a future injury in order to comply with [the injury-in-fact] requirement, but only if he or she "is *immediately* in danger of sustaining some *direct* injury as a result of the challenged

---

the Earth, Inc. v. Gaston Copper Recycling Corp., 204 F.3d 149, 160 (en banc) (holding that "[t]hreats or increased risk . . . constitutes cognizable harm")).

78. *See id.* at 634 n.4 (citing Lac Du Flambeau Band of Lake Superior Chippewa Indians v. Norton, 422 F.3d 490, 498 (7th Cir. 2005) (holding that the approval of a gaming contract between the State of Wisconsin and the Ho-Chunk Nation presented the plaintiffs with a future though uncertain harm that established an injury-in-fact for standing purposes); Johnson v. Allsteel, Inc., 259 F.3d 885, 888 (7th Cir. 2001) (finding that an ERISA plan administrator's increased discretionary powers presented an increased risk that the plaintiff would be denied benefits, and that "[t]he increased risk the participant faces as a result is an injury-in-fact" for standing purposes); Vill. of Elk Grove Vill. v. Evans, 997 F.2d 328, 329 (7th Cir. 1993) (In a suit brought by municipal officials to enjoin the U.S. Army Corps of Engineers from granting a permit for the construction of a radio tower, the court stated that "even a small probability of injury is sufficient to create a case or controversy–to take a suit out of the category of the hypothetical–provided of course that the relief sought would, if granted, reduce the probability.").

79. *Pisciotta*, 499 F.3d at 634.

80. *See* Krottner v. Starbucks Corp., 628 F.3d 1139, 1143 (9th Cir. 2010).

81. *Id.* at 1140.

82. *Id.* at 1141.

83. *Id.* at 1143.

84. *Id.* at 1142–43.

> . . . conduct and the injury or threat of injury is both real and immediate, not conjectural or hypothetical."[85]

In the court's mind, the theft of the laptop containing the plaintiffs' personal information caused them immediate danger of a direct injury, meeting the "actual or imminent" requirement for standing.[86]

At least one district court outside the jurisdiction of the Seventh and Ninth Circuits has taken notice of these decisions. In *Caudle v. Towers, Perrin, Forster & Crosby, Inc.*, the Social Security numbers of thousands of Altria[87] employees were compromised when several laptops were stolen from the New York office of their employer's pension consultant.[88] When the consultant informed the plaintiffs of the breach, it noted that only "some" of the files containing the personal information were password-protected.[89] The consultant also arranged for all those affected to enroll in two years of free Equifax credit monitoring, but the plaintiffs instead decided to pursue the matter through the courts.[90] Relying on *Pisciotta*, the court concluded that the standing requirement was satisfied.[91] Like the *Pisciotta* court, the *Caudle* court analogized the future risk of personal injury to a case involving exposure to environmental toxins,[92] noting that the potential harm caused by exposure to identity theft, like exposure to dangerous substances, may result in an unreasonable exposure causing a cognizable injury.[93] However, two years later the same court came to a different

85. *Id.* at 1142 (quoting Scott v. Pasadena Unified Sch. Dist., 306 F.3d 646, 656 (9th Cir. 2002)).

86. *Id.* at 1143.

87. Altria is the parent company of Philip Morris USA, the largest tobacco company in the United States. *See About Philip Morris USA*, PHILLIPMORRISUSA, http://www.philipmorrisusa.com/en/cms/Company/Corporate_Structure/default.aspx?src=home (last visited Oct. 2, 2011).

88. Caudle v. Towers, Perrin, Forster & Crosby, Inc., 580 F. Supp. 2d 273, 275–76 (S.D.N.Y. 2008).

89. *Id.* at 276 (citing Caudle Dep. at 12).

90. *Id.* Equifax bills itself as a global leader in information solutions, able to leverage sources of consumer and commercial data "to create customized insights that enrich both the performance of businesses and the lives of consumers." *About Equifax: Company Profile*, EQUIFAX, http://www.equifax.com/about_equifax/company_profile/en_us (last visited Sept. 29, 2011). Equifax claims to "empower individual consumers to manage their personal credit information, protect their identity, and maximize their financial well-being." *Id.*

91. *Caudle*, 580 F. Supp. 2d at 279–80.

92. *Id.* at 279 (citing LaFleur v. Whitman, 300 F.3d 256, 270 (2d Cir. 2002) (holding that exposure to sulfur dioxide emissions qualifies as an injury-in-fact sufficient to confer standing)).

93. *Id.* at 279–80 (citing Baur v. Veneman, 352 F.3d 625, 634 (2d Cir. 2003)).

conclusion in *Hammond*[94] and chose to distinguish itself from *Caudle* based on the underlying facts of the case.[95]

In sum, although some courts have recently been willing to grant standing in cases involving the inadequate storage of personal information, it is clear that the issue is far from settled. Many courts have thus far refused to allow these cases to be heard on the merits, leaving the affected citizens with no judicial redress. As this sort of information is increasingly stored on a massive scale, there needs to be some way to ensure that these types of individuals have access to the courthouse door. In many jurisdictions, the mere filing of this type of complaint continues to be a non-starter.

B. *The Difficulty in Proving Damages*

Those plaintiffs fortunate enough to move past the standing hurdle may then find themselves at another impasse: proving their damages suffered, down to a specific monetary number. Realizing that one's personal information has been compromised can certainly cause a fair amount of emotional distress, but without definitive proof that this information has actually been misused, courts have been reluctant to quantify this type of loss. The cost of subscribing to some sort of credit monitoring agency may be easy to prove, but whether this should count toward a plaintiff's total damages is treated differently among the courts. Just like the question of standing, courts have taken divergent positions on both these issues.

To date, the Ninth Circuit appears to be the only federal circuit court to address the issue of damages within the personal electronic data context.[96] In *Ruiz v. Gap, Inc.*, a thief gained access to the offices of a vendor that processed Gap's job applications and stole two laptops.[97] At the time, one of the computers was downloading information about Gap job applicants and contained the Social Security numbers and other personal information of approximately 750,000 persons.[98] Gap notified all applicants whose personal information was on the computer and offered to provide one year of credit monitoring

94. Hammond v. Bank of N.Y. Mellon Corp., No. 08 Civ. 6060(RMB)(RLE), 2010 WL 2643307, at *2 (S.D.N.Y. June 25, 2010) (concluding, unlike the *Caudle* court, that the plaintiffs lacked standing entirely because "they claim to have suffered little more than an increased risk of future harm from the loss (whether by accident or theft) of their personal information.").

95. *See id.* at *4–6.

96. *See* Ruiz v. Gap, 380 F. App'x 689 (9th Cir. 2010).

97. Because *Ruiz* is an unpublished opinion, the facts of *Ruiz* are not discussed within the court's opinion. The court merely states that "Because the parties are familiar with the facts and procedural history, we need not recount it here." *Ruiz*, 380 F. App'x at 690. For a discussion of the facts, *see* Proskauer Rose LLP, *California District Court Closes the Gap Left by Ruiz*, PROSKAUER PRIVACY LAW BLOG (Apr. 9, 2009), http://privacylaw.proskauer.com/2009/04/articles/data-breaches/california-district-court-closes-the-gap-left-by-ruiz/.

98. Proskauer Rose LLP, *supra* note 97.

for free.[99] Unsatisfied with this offer, one of the job applicants filed a class action suit alleging negligence, breach of contract, and invasion of privacy under a California statute.[100]

In an unpublished opinion, the Ninth Circuit Court of Appeals affirmed the summary judgment granted to the defense by the trial court.[101] Although it affirmed the trial court's finding that Ruiz had standing to pursue his claims, the Ninth Circuit found that he had not established "sufficient appreciable, non-speculative, present harm" with regards to his negligence claim.[102] Relying on a previous California case which found that "[n]ominal damages, to vindicate a technical right, cannot be recovered . . . where no actual loss has occurred," it held that the plaintiff's increased susceptibility to identity theft could not be given monetary value at that time.[103] With regard to Ruiz's damages based on the time and money he had spent to monitor his credit, the court stated that this issue was a matter of first impression.[104] However, since the plaintiff had offered no evidence as to the value of these damages and offered no evidence that Gap's offer would not fully compensate his losses, the court upheld the dismissal of the case.[105]

The United States District Court for the District of Connecticut has also rejected plaintiffs' claims with respect to damages after finding a sufficient basis to confer standing.[106] In another case arising out of the loss of Bank of New York Mellon's back-up tapes,[107] the plaintiffs on appeal claimed that their damages came in the form of fees paid to the defendants for preventing the misuse of their personal banking and financial information.[108] Although they admitted there was an absence of any quantifiable loss due to this increased risk of misuse, the plaintiffs analogized their injuries to the damages resulting from faulty tax advice.[109] The plaintiffs theorized that this increased risk of identity theft and misuse of personal information was sufficient to es-

99. *Id.*

100. *See Ruiz*, 380 F. App'x at 689–91.

101. *Id.* at 693.

102. *Id.* at 691.

103. *Id.* (quoting Fields v. Napa Milling Co., 330 P.2d 459, 462 (Cal. Ct. App. 1958)).

104. *See id.*

105. *Id.*

106. *See* McLoughlin v. People's United Bank, Inc., No. 3:08-cv-0944(VLB), 2009 WL 2843269, at *4, *8 (D. Conn. Aug. 31, 2009).

107. *See* Hammond v. Bank of N.Y. Mellon Corp., No. 08 Civ. 6060(RMB)(RLE), 2010 WL 2643307, at *2 (S.D.N.Y. June 25, 2010); *supra* Part II.A.

108. *McLoughlin*, 2009 WL 2843269, at *3.

109. *Id.* (citing Denney v. Deutsche Bank AG, 443 F.3d 253, 264–65 (2d Cir. 2006)). In *Denney v. Deutsche Bank AG*, the plaintiffs alleged damages resulting from the payment of excessive fees for faulty tax advice. *Denney*, 443 F.3d at 264–65. In addition to the increased risks of being audited, the plaintiffs alleged that they had foregone certain tax benefits and had taken "costly and time-consuming steps" to rectify the errors caused by the defendant's negligence. *Id.*

tablish actual damages and that they should have the right to prove these damages at trial.[110]

Although the injuries alleged were sufficient to confer standing, the court dismissed the case based on the plaintiff's inability to prove actual damages.[111] Following the Connecticut Supreme Court, it held that "'conduct that is merely negligent, without proof of an actual injury, is not considered to be a significant interference with the public interest such that there is any right to complain of it, or be free from it.'"[112] The plaintiffs, meanwhile, were unable to point to any case law allowing a negligence claim to survive absent allegations of actual identity theft.[113] The court therefore refused to allow the claim to go forward solely based on the fear of identity theft resulting from the plaintiffs' injuries and dismissed the case.[114]

A federal court in Minnesota reached a similar result.[115] In *Forbes v. Wells Fargo Bank*, computers containing the names, addresses, Social Security numbers, and account numbers of Wells Fargo mortgage customers were stolen from the computers of a company hired by the defendant.[116] In their notification to the affected customers, Wells Fargo offered free informational and identity protection services.[117] Although there was no indication that any of the stolen information had been misused, some customers decided to file suit for breach of contract and negligence based upon the time and money they had personally spent monitoring their credit for fraud.[118]

The district court found that the plaintiffs had standing to bring the suit but dismissed both claims at the summary judgment stage.[119] Like the Connecticut court, the Minnesota court held that the threat of a future harm that has yet to be realized cannot satisfy the requirement to prove damages under both claims.[120] Although it noted that a plaintiff may recover for the losses of time in terms of earning capacity,[121] the court found that the plaintiff's time spent monitoring their credit was not the result of a present injury, but rather "the anticipation of future injury that has not materialized."[122] Because the plain-

110. *See McLoughlin*, 2009 WL 2843269, at *7–8.
111. *Id.* at *7–9.
112. *Id.* at *8 (quoting Right v. Breen, 890 A.2d 1287, 1294 (Conn. 2006)).
113. *Id.*
114. *See id.* at *8–9.
115. *See* Forbes v. Wells Fargo Bank, N.A., 420 F. Supp. 2d 1018, 1021 (D. Minn. 2006).
116. *Id.* at 1019.
117. *Id.*
118. *Id.* at 1019–20.
119. *See id.* at 1021.
120. *Id.* at 1020 (quoting Reliance Ins. Co. v. Arneson, 322 N.W.2d 604, 607 (Minn. 1982)).
121. *Id.* at 1020–21 (citing Cox v. Chicago Great W. R.R. Co., 223 N.W. 675, 677 (1929)).
122. *Id.* at 1021.

tiffs could not show support for damages resulting from an injury that was reasonably certain to occur, they failed to establish a necessary element of both their negligence and breach of contract claims, and the defendant's motion for summary judgment was granted.[123]

After conferring standing, the court in *Caudle v. Towers, Perrin, Forster & Crosby*, went on to dismiss the plaintiffs' negligence claim.[124] With respect to his breach of contract claim, however, the court found that the plaintiff had sufficiently demonstrated that he was a third-party beneficiary to the contract between Towers and his employer, Altria, at least for purposes of a summary judgment motion.[125] Although the plaintiff had been offered one free year of credit monitoring with an established vendor,[126] he sought the cost of purchasing a lifetime insurance policy covering any misuse resulting from the theft of his personal information, as well as the cost of monitoring.[127] The court ultimately left the issue of deciding damages for another day and ordered more discovery as to whether the plaintiff was a third-party beneficiary under the contract between Towers and Altria.[128]

Finally, the Northern District of California has at least given credence to the idea that plaintiffs should be provided more than a token value for another party's loss of their personal information.[129] In the *TD Ameritrade* litigation, the financial company's online security system was exploited by hackers, and the private information of 6.3 million customers was stolen.[130] Although financial information and Social Security numbers were not among the hacked data, the theft did render the customers vulnerable to spamming, telephone solicitations, and direct mail marketing.[131]

After a class action lawsuit was filed, the parties entered into settlement negotiations.[132] Under the proposed settlement offer, TD Ameritrade agreed to give all affected customers a one-year subscription to anti-virus and spam-blocking software, among other concessions.[133] The lawyers involved told the judge that TD Ameritrade would be spending approximately $10 million on the deal, including $6

123. *Id.*

124. Caudle v. Towers, Perrin, Forster & Crosby, Inc., 580 F. Supp. 2d 273, 282 (S.D.N.Y. 2008).

125. *Id.* at 284.

126. *Id.* at 281 n.2.

127. *Id.* at 281.

128. *Id.* at 284.

129. *See In re* TD Ameritrade Accountholder Litig., 266 F.R.D. 418, 424 (N.D. Cal. 2009).

130. Kravets, *supra* note 6; *In re* TD Ameritrade, 266 F.R.D. at 419.

131. The hackers were able to steal the customers' names, phone numbers, email accounts, and home addresses of 6.5 million TD Ameritrade customers. Kravets, *supra* note 6; *see In re* TD Ameritrade, 266 F.R.D. at 419.

132. *In re TD Ameritrade*, 266 F.R.D. at 419.

133. The court listed the concessions of TD Ameritrade as follows:

million for the anti-virus and anti-spamming software.[134] Meanwhile, the lawyers involved in the deal would receive $1.87 million.[135] In total, the deal would work out to a payment of less than $2 per victim, which came in the form of free software.[136] One attorney in particular objected to the settlement arguing that the potential harm to class members resulting from an increased risk of identity theft was not adequately compensated under the proposed settlement.[137]

The court decided to reject the settlement.[138] It noted that the settlement did not require TD Ameritrade to adopt any new permanent security measures and that tests of the network should, in any case, be "routine practice" for "a large company that deals in sensitive personal information."[139] More importantly, the court held that the proposed settlement sought to confer "no discernable benefit upon the class" and left the class "with nothing."[140] Most Internet users would be able to obtain the proposed software for little to no cost, and the rest of the settlement provisions were mainly for the benefit of TD Ameritrade itself.[141] While the court did not put its own monetary figure on the amount of the harm caused to the plaintiffs, it clearly accepted the notion that the value of the damages in this case was more than the cost of a one-year software subscription.[142]

Although some courts have allowed plaintiffs whose personal information has been compromised to bring suit, the case law makes one thing clear: individuals have no general, freestanding right to have their personal data stored securely. The emotional trauma and time

---

In return for the class dropping its claims against TD Ameritrade, TD Ameritrade offered to (1) post a warning on its website "regarding stock spam"; (2) "continue to retain independent experts" to test TD Ameritrade's security vulnerabilities; (3) continue "account seeding" to determine whether unauthorized persons have acquired customer email addresses; (4) provide each settlement class member with a unique identifier number that can be used to obtain a one-year subscription to an anti-virus, anti-spam internet security product; (5) retain a company to perform an analysis to determine whether any incidents of organized misuse of personal information had occurred involving data in the TD Ameritrade database (four such analyses already had been performed) and to inform settlement class members whose personal information is discovered to be the subject of organized misuse; (6) donate $55,000 to specified cyber-security projects; and (7) pay claims administration and notice expenses for the settlement.

Id. at 420.

134. *See* Kravets, *supra* note 6.

135. *In re TD Ameritrade*, 266 F.R.D. at 420.

136. Kravets, *supra* note 6.

137. *See In re TD Ameritrade*, 266 F.R.D. at 419–20 (noting that the Texas Attorney General had intervened in the case on behalf of Texas accountholders and objected to the settlement proposal for various reasons).

138. *See id.* at 424.

139. *Id.* at 422.

140. *Id.* at 422–23.

141. *See id.* at 420, 422–23.

142. *See id.* at 422–24.

spent furiously monitoring email, financial accounts, and other data in anticipation of misuse or fraud is currently a cost that the legal system is seemingly unwilling to quantify.

However, the damage caused by the failure to adequately secure this type of information is real. There must be a way to ensure that those people affected by an electronic breach of their personal information can find adequate redress through the court system. Part of the solution to this growing problem must therefore include a private cause of action, which does not require the plaintiff to prove actual identity theft or misuse. By allowing these individuals redress through the courts, entities that fail to adequately store this type of information may be held accountable for their actions, and therefore will have a tremendous incentive to protect the personal data they keep.

III. THE CURRENT FEDERAL STATUTORY FRAMEWORK AND RECENT STATE LEGISLATION MANDATING THE ENCRYPTION OF PERSONAL INFORMATION

Individuals whose personal information is lost or stolen have thus far been bringing suit under common law claims of negligence and breach of contract because both federal and state law are woefully inadequate. Although the federal government has a number of laws on the books dealing with the transmission of personal information,[143] most are directed at penalizing the person who actually accesses or misuses the information, and some are all but obsolete in the digital age. Current laws do very little to penalize the individual or organization that failed to adequately secure the information in the first place. Most states have a data breach law but only require the organization to *notify* the affected individuals whose personal information was lost or stolen.[144] These laws only penalize entities if they fail to report the

143. *See generally* Computer Fraud & Abuse Act, 18 U.S.C.A. § 1030 (West 2000 & Supp. 2011); Electronic Communications Privacy Act of 1986, 18 U.S.C.A. §§ 2510–2522 (West 2000 & Supp. 2011); Fair and Accurate Credit Transactions Act of 2003, Pub. L. No. 108-159, 117 Stat. 1952; Fair Credit Reporting Act, 15 U.S.C. § 1681 (2006).

144. *See* ALASKA STAT. § 45.48.010 (2010); ARIZ. REV. STAT. ANN. § 44-7501 (Supp. 2010); ARK. CODE ANN. § 4-110-105 (Supp. 2011); CAL. CIV. CODE § 1798.82 (West 2009); COLO. REV. STAT. § 6-1-716 (2011); CONN. GEN. STAT. § 36a-701b (Supp. 2011); DEL. CODE ANN. tit. 6, § 12B-102 (2005); D.C. CODE § 28-3852 (Supp. 2011); FLA. STAT. § 817.5681 (2005); GA. CODE ANN. § 10-1-912 (2005); HAW. REV. STAT. ANN. § 487N-2 (LexisNexis 2009); IDAHO CODE ANN. § 28-51-105 (Supp. 2011); 815 ILL. COMP. STAT. ANN. 530/5–30 (West 2008); IND. CODE ANN. §§ 24-4.9-3-1 to -2 (West Supp. 2011); IOWA CODE ANN. §§ 715C.1–.2 (West Supp. 2011); KAN. STAT. ANN. § 50-7a02 (Supp. 2009); LA. REV. STAT. ANN. § 51:3074 (Supp. 2011); ME. REV. STAT. ANN. tit. 10, § 1348 (2009 & Supp. 2010); MD. CODE ANN., COM. LAW §§ 14-3501 to -3508 (LexisNexis Supp. 2010); MASS. GEN. LAWS ANN. ch. 93H, § 3 (West Supp. 2011); MICH. COMP. LAWS ANN. § 445.72 (West Supp. 2011); MINN. STAT. ANN. § 325E.61 (West 2011); MONT. CODE ANN. § 30-14-1704 (2009); NEB. REV. STAT. ANN. §§ 87-801 to -807 (LexisNexis 2007); NEV. REV. STAT. ANN. §§ 603A.010–.920 (LexisNexis 2010); N.H. REV. STAT. ANN. § 359-C:19 (2009); N.J.

breach and do nothing to create some sort of uniform standard to prevent the loss or theft of such information in the first place.

Several states, however, have taken the lead by requiring certain encryption standards to be met when storing large amounts of personal information electronically.[145] Massachusetts and Nevada have both enacted laws that require the encryption of personal information, and they provide penalties for failure to comply with these standards. Bills have also been introduced at the federal level, including most recently the Rush Bill in the House[146] and the Pryor and Rockefeller Bill in the Senate,[147] but neither of these bills appears to have much chance of becoming law. By looking at the current statutory framework across the United States, it is easy to see why a new national law is needed, and the examples in Massachusetts and Nevada provide a great model that can be implemented at the federal level.

A. *Why Current Federal Legislation is Inadequate*

The federal laws already on the books cannot be adapted to address the personal hardship caused by companies that fail to secure personal information. Many have sections addressing the problems associated with hacking, but do very little in the way of helping individuals who might be affected.

Take, for instance, the Electronic Communications Privacy Act ("ECPA").[148] The ECPA makes it a crime for anyone to intentionally intercept or unlawfully obtain electronic messages either stored or in the process of transmission.[149] Under the part of the act discussing stored communications, the statute provides for a civil cause of action.[150] The statute also provides for a minimum of $1,000 of damages

---

STAT. ANN. § 56:8-163 (Supp. 2011); N.Y. GEN. BUS. LAW § 899-aa (Supp. 2011); N.C. GEN. STAT. § 75-65 (2009); N.D. CENT. CODE § 51-30-02 to -03 (2007); OKLA. STAT. ANN. tit. 74, § 3113.1 (Supp. 2010); OHIO REV. CODE ANN. § 1349.19(B)(1) (LexisNexis 2006 & Supp. 2011); OR. REV. STAT. § 646A.600–.628 (2009); 73 PA. CONS. STAT. ANN. § 2303 (West 2008); R.I. GEN. LAWS § 11-49.2-3 (Supp. 2010); S.C. CODE ANN. § 39-1-90(A) (Supp. 2010); TENN. CODE ANN. § 47-18-2107 (Supp. 2011); TEX. BUS. & COM. CODE ANN. §§ 521.051, 521.053 (West Supp. 2010); UTAH CODE ANN. § 13-44-202 (LexisNexis 2009); VT. STAT. ANN. tit. 9, § 2435 (Supp. 2010); VA. CODE ANN. § 18.2-186.6 (2008); WASH. REV. CODE § 19.255.010 (2005); W. VA. CODE § 46A-2A-102 (Supp. 2011); WIS. STAT. § 134.98 (2006); WYO. STAT. ANN. § 40-12-509 (2007).

145. *See* Security of Personal Information, NEV. REV. STAT. ANN. § 603A.215 (LexisNexis 2010); 201 MASS. CODE REGS. 17.04 (2008).

146. *See* Data Accountability and Trust Act, H.R. 2221, 111th Cong. (2009).

147. *See* Data Security and Breach Notification Act, S. 3742, 111th Cong. (2010).

148. 18 U.S.C.A. §§ 2510–2522 (West 2000 & Supp. 2011). The ECPA consists of the Wiretap Act, 18 U.S.C. §§ 2510–2522 (West 2000 & Supp. 2011), and the Stored Communications Act, 18 U.S.C. §§ 2701–2712 (West 2000 & Supp. 2011).

149. *See* § 2511(1) (2000).

150. *See* § 2707.

for each violation, but the aggrieved party is entitled to recover more if he or she can prove actual damages greater than $1,000.[151]

The problem with the ECPA in our context is that it limits who is entitled to bring suit. The relevant section states that "any provider of [an] electronic communication service, subscriber, or other person aggrieved by any violation" may bring forth a civil action to recover damages.[152] Under the definitions, an "aggrieved person" means "a person who was a *party* to any intercepted wire, oral, or electronic communication or a person against whom the interception was directed."[153] In the criminal context, courts have previously held that a defendant who was not actually a party to a communication may not be considered an "aggrieved person," even though the defendant was affected by the interception.[154] So the owner of a website or server whose database of personal information was stolen is entitled to recover under the ECPA, but the *individual* whose information was compromised does not have a right to bring suit. The individual does not qualify as a party to the interception unless it can be shown that the theft of the information occurred as it was being provided by or to the individual over the Internet in real time.

Another law addressing the problem of electronic identity theft is the Fair and Accurate Credit Transactions Act of 2003 ("FACTA").[155] The most well-known provision in FACTA is the provision that allows consumers to obtain an annual free credit report.[156] In addition, FACTA does take some steps to address the problems associated with identity theft. Section 114 requires financial institutions to implement programs to prevent identity theft,[157] while another section prohibits consumer reporting agencies from furnishing medical information about a consumer, with limited exceptions.[158] Section 113 of FACTA also requires businesses to truncate the credit card and debit card numbers of their customers on printed receipts but says nothing about the electronic storage of this type of information.[159] Any agency that fails to undertake any of these requirements may be held civilly liable by a consumer for up to $1,000 in actual damages and may be awarded punitive damages as the court may allow.[160]

---

151. *See* § 2707(c).
152. § 2707(a).
153. § 2510(11) (emphasis added).
154. *See* United States v. Fury, 554 F.2d 522, 525 (2d Cir. 1977); *In re* Berry, 521 F.2d 179, 185 (10th Cir. 1977).
155. *See* Pub. L. No. 108-159, 117 Stat. 1952; Fair and Accurate Credit Transactions Act of 2003, Pub. L. No. 108-159, 117 Stat. 1952 (codified as amended at 15 U.S.C. § 1681 (2006)).
156. Fair and Accurate Credit Transactions Act of 2003, § 211 (codified as amended at 15 U.S.C. § 1681j(a)(1)(A) (2006)).
157. *Id.* at §114 (codified as amended at 15 U.S.C. § 1681 (2006)).
158. *See id.* § 411.
159. *See id.* § 113.
160. 15 U.S.C. § 1681n(a).

Although FACTA requires financial institutions to take affirmative steps to prevent identity theft, its provisions are too narrow to be an all-encompassing solution. The act provides for a right of recovery in court, but the plaintiff must be able to prove actual damages. As the case law discussed shows, this is extremely difficult where actual identity theft has not yet occurred. FACTA is also limited to financial institutions that obtain personal financial information and does not explicitly cover other information such as Social Security numbers or home addresses. Most importantly, FACTA does not have any provisions that discuss the security of financial information stored in an electronic format. While truncating credit card numbers on printed receipts is a step in the right direction, it does not address the vulnerability of this information when stored electronically. A financial institution's identity theft prevention program would presumably include the electronic storage of information, but FACTA fails to address this concern explicitly, and is therefore written too narrowly to fully address the problem.

The Computer Fraud and Abuse Act ("CFAA" or "Act")[161] is perhaps most able to address the harm caused by failure to protect personal information, but it too is not without flaws. Under the Act, it is a crime to "intentionally access[ ] a computer without authorization" and obtain "information contained in a financial record of a financial institution" or "information from any protected computer."[162] A protected computer is defined as follows:

> The term "protected computer" means a computer (A) exclusively for the use of a financial institution of the United States Government, or, in the case of a computer not exclusively for such use, used by or for a financial institution or the United States Government and the conduct constituting the offense affects that use by or for the financial institution or the Government; or (B) which is used in or affecting interstate or foreign commerce or communication, including a computer located outside the United States that is used in a manner that affects interstate or foreign commerce or communication of the United States.[163]

The statute also defines a "financial institution" to include banks, credit unions, brokers, and any institution of the Farm Credit System.[164]

Anyone who violates the CFAA may face a fine and up to five years imprisonment if the offense was committed "for purposes of commercial advantage or private financial gain"[165] or if "the value of the in-

161. 18 U.S.C.A. § 1030 (West 2000 & Supp. 2011).

162. *See* §1030(a)(2).

163. § 1030(e)(2).

164. *See* § 1030(e)(4).

165. § 1030(c)(2)(B)(i).

formation obtained exceeds $5,000."[166] Importantly, the statute also provides for a private right of recovery:

> Any person who suffers damage or loss by reason of a violation of this section may maintain a civil action against the violator to obtain compensatory damages and injunctive relief or other equitable relief . . . . Damages for a violation involving only conduct described in (c)(4)(A)(i)(I)[167] are limited to economic damages.[168]

Any person bringing an action under this section has a two-year statute of limitations from the time the damage is discovered.[169]

The CFAA has been invoked from time to time by plaintiffs who have lost sensitive information and sustained damages.[170] However, the Act does not address all the concerns regarding the protection of personal information stored electronically. While the Act penalizes the unlawful access of a protected computer, it does not provide a prescription for preventing these types of losses in the first place. Furthermore, while hacking is clearly addressed under the statute, recent case law suggests that less sophisticated forms of data theft would not be covered. Last year, the Eastern District of Wisconsin held that an employee of a credit union did not violate the CFAA after accessing her company's files following her resignation.[171] Similarly, the District of Maryland has held that employees who freely accessed their company's electronic information and subsequently misused the information for personal financial gain were not in violation of the CFAA.[172] Applying these cases, it would also seem likely that obtaining personal information through the use of a laptop with unencrypted files would not constitute a CFAA violation. If so, then this would seem to be a fairly wide loophole that the CFAA fails to address.

It is also questionable whether a person whose personal information was stored with an entity who then loses the data would be considered "a person who suffers damage or loss" under the CFAA. Two circuit courts have previously held that the CFAA does not restrict consideration of losses to the person who actually owned the computer system.[173] However, any losses considered must be limited to *economic*

166. § 1030(c)(2)(B)(iii).

167. § 1030(c)(4)(A)(i)(I) ("loss to 1 or more persons during any 1-year period . . . aggregating at least $5,000 in value.").

168. § 1030(g).

169. *Id.*

170. *See, e.g.*, United States v. Middleton, 231 F.3d 1207, 1208 (9th Cir. 2000); Spangler, Jennings & Dougherty, P.C. v. Mysliwy, No. 2:05-cv-00108-JTM-APR (N.D. Ind. Mar. 31, 2006).

171. *See* Landmark Credit Union v. Doberstein, 746 F. Supp. 2d 990, 993–94 (E.D. Wis. 2010).

172. *See* Océ N. Am., Inc. v. MCS Servs., Inc., 748 F. Supp. 2d 481, 485–87 (D. Md. 2010).

173. *See* United States v. Millot, 433 F.3d 1057, 1061 (8th Cir. 2006); Theofel v. Farey Jones, 341 F.3d 978, 986 (9th Cir. 2003).

damages of at least $5,000.[174] While courts have held that these may include the cost of restoring the data, responding to the offense, and any revenues lost,[175] there is a narrow range of economic activity for which the CFAA provides a right to recovery. In our context, economic damages would only include the losses sustained as a result of actual identity theft. People who suffer only from the knowledge that their personal information was compromised will continue to be left without remedy.

Upon review of the current federal law, it is clear that additional legislation is needed to specifically address injuries beyond actual identity theft. Business and organizations that fail to properly store personal information electronically should be held liable when this data is hacked or otherwise lost. Statutory, not just economic, damages should be available to the persons affected by these types of data breaches because the current federal statutory landscape is unable to provide adequate redress. Statutes such as the CFAA and FACTA are a good start, but in the end are too narrowly tailored to fit the specific problems that often occur when storing personal data electronically.

B. *State Laws and Proposed Federal Legislation Providing a Model for National Reform*

Some federal legislation has been proposed that seeks to address this issue, but so far, Congress has failed to act.[176] A couple of states, however, have taken the lead and now have laws on the books requiring certain data to be encrypted,[177] including personal information held by businesses. Here, we will look at the recently enacted legislation in Massachusetts and Nevada, and consider how these laws may provide an example for national reform on this issue.

1. State Notification Laws

Forty-five states currently have laws dealing with the unauthorized access and acquisition of personal information stored electronically.[178]

174. *See* §1030(g).

175. *See Middleton*, 231 F.3d at 1213.

176. Data Accountability and Trust Act, H.R. 2221, 111th Cong. (2009); Data Security and Breach Notification Act, S. 3742, 111th Cong. (2010).

177. *See* Security of Personal Information, NEV. REV. STAT. ANN. § 603A.210 (LexisNexis 2010); 201 MASS. CODE REGS. 17.04 (2008).

178. ALASKA STAT. §§ 45.48.010–.090 (2010); ARIZ. REV. STAT. ANN § 44-7501 (Supp. 2010); ARK. CODE ANN. §§ 4-110-101 to -108 (Supp. 2011); CAL. CIV. CODE § 1798.82 (West 2009); COLO. REV. STAT. § 6-1-716 (2011); CONN. GEN. STAT. § 36a-701b (Supp. 2011); DEL. CODE ANN. tit. 6, §§ 12B-101 to -104 (2005); D.C. CODE §§ 28-3851 to -3852 (Supp. 2011); FLA. STAT. § 817.5681 (2005); GA. CODE ANN. §§ 10-1-911 to -912 (2005); HAW. REV. STAT. ANN. §§ 487N-1 to -7 (LexisNexis 2009); IDAHO CODE ANN. §§ 28-51-104 to -107 (Supp. 2011); 815 ILL. COMP. STAT. ANN. 530/5–30 (West 2008); IND. CODE ANN. §§ 24-4.9-1-1 to -3-3.5 (West Supp. 2011); IOWA CODE ANN. §§ 715C.1–.2 (West Supp. 2011); KAN. STAT. ANN. §§ 50-7a01 to -

However, these statutes are more concerned with requiring entities to notify the individuals affected than they are with creating a uniform system to prevent access in the first place.

The Virginia Breach of Personal Information Notification law provides a typical example.[179] Under Virginia law, entities that maintain a database of personal information[180] are required to provide notice to both the individuals affected and the Attorney General should the information be compromised.[181] Notice must be made to the affected individuals "without unreasonable delay"[182] and can be made in writing, by telephone, or by email.[183]

The problem with these types of laws that exist all across the country is that they only require *notice* in the event personal information is compromised. The Virginia statute even refers to information acquired in both "encrypted and unencrypted" form,[184] making it clear that the method of storing this type of data should be left to the entities themselves. The Virginia Attorney General has the right to impose a civil penalty of up to $150,000, but only in the event that an entity fails to notify the required parties.[185] Statutes like that in Virginia provide a good first step, but they lack the teeth needed to spur a change in the way personal data is kept.

7a02 (Supp. 2009); LA. REV. STAT. ANN. §§ 51:3071–77 (Supp. 2011); ME. REV. STAT. ANN. tit. 10, §§ 1346 to 1350-B (2009 & Supp. 2010); MD. CODE ANN., COM. LAW §§ 14-3501 to -3508 (LexisNexis Supp. 2010); MASS. GEN. LAWS ANN. ch. 93H, §§ 1–6 (West Supp. 2011); MICH. COMP. LAWS ANN. § 445.72 (West Supp. 2011); MINN. STAT. ANN. § 325E.61 (West 2011); MONT. CODE ANN. § 30-14-1704 (2009); NEB. REV. STAT. ANN. §§ 87-801 to -807 (LexisNexis 2007); NEV. REV. STAT. ANN. §§ 603A.010–.220 (LexisNexis 2010); N.H. REV. STAT. ANN. § 359-C:19 (2009); N.J. STAT. ANN. § 56:8-163 (Supp. 2011); N.Y. GEN. BUS. LAW § 899-aa (Supp. 2011); N.C. GEN. STAT. §§ 75-60 to -65 (2009); N.D. CENT. CODE § 51-30-01 to -07 (2007); OKLA. STAT. ANN. tit. 74, § 3113.1 (Supp. 2010); OHIO REV. CODE ANN. § 1349.19 (LexisNexis 2006 & Supp. 2011); OR. REV. STAT. § 646A.600–.628 (2009); 73 PA. CONS. STAT. ANN. § 2303 (West 2008); R.I. GEN. LAWS § 11-49.2-3 (Supp. 2010); S.C. CODE ANN. § 39-1-90 (Supp. 2010); TENN. CODE ANN. § 47-18-2107 (Supp. 2011); TEX. BUS. & COM. CODE ANN. §§ 521.051–.053 (West Supp. 2010); UTAH CODE ANN. § 13-44-202 (LexisNexis 2009); VT. STAT. ANN. tit. 9, § 2435 (Supp. 2010); VA. CODE ANN. § 18.2-186.6 (2008); WASH. REV. CODE § 19.255.010 (2005); W. VA. CODE § 46A-2A-101 to -105 (Supp. 2011); WIS. STAT. § 134.98 (2006); WYO. STAT. ANN. § 40-12-509 (2007).

179. VA. CODE ANN. § 18.2-186.6 (2008).

180. § 18.2-186.6(A) (defining "personal information" to include "the first name or first initial and last name" of a person in combination with their Social Security number, driver's license number, or a financial account number).

181. § 18.2-186.6(B).

182. *Id.*

183. § 18.2-186.6(A).

184. *See* § 18.2-186.6(C).

185. *See* § 18.2-186.6(I).

2. The Nevada Model

The Security of Personal Information law enacted in Nevada in 2008 was the first law in the country to require the encryption of personal data.[186] As of October 1, 2008, Nevada made it mandatory for all data collectors to encrypt personal information. A "data collector" is defined under the code to include "any governmental agency, institution of higher education, corporation, financial institution or retail operator or any other type of business entity or association that, for any purpose, whether by automated collection or otherwise, handles, collects, disseminates, or otherwise deals with nonpublic personal information."[187] As in Virginia, personal information is considered to be a person's first name or first initial and last name in combination with his or her Social Security number; driver's license number; or account number, credit card number, or debit card number "in combination with any security code, access code, or password."[188] This means that companies that maintain credit card information but not the corresponding security codes—such as convenience stores and in-person retailers—are not considered data collectors under Nevada law.[189]

One of the more interesting aspects of the Nevada model is its requirement that all files containing personal information must be encrypted. Encryption is defined as follows:

> "Encryption" means the protection of data in electronic or optical form, in storage or in transit, using:
>
> (1) An encryption technology that has been adopted by an established standards setting body, including, but not limited to, the Federal Information Processing Standards issued by the National Institute of Standards and Technology, which renders such data indecipherable in the absence of associated cryptographic keys necessary to enable decryption of such data; and
>
> (2) Appropriate management and safeguards of cryptographic keys to protect the integrity of the encryption using guidelines promulgated by an established standards setting body, including, but not limited to, the National Institute of Standards and Technology.[190]

---

186. Sushila Nair, *Data Breach Disclosure in the USA: An Emerging Framework Around Data Security*, SECURECOMPLIANCE (Feb. 4, 2010, 2:50 PM), http://www.btsecurethinking.com/tag/nevada-security-law/; *see* Security of Personal Information, NEV. REV. STAT. ANN. § 603A (LexisNexis 2010).

187. NEV. REV. STAT. ANN. § 603A.030 (LexisNexis 2010).

188. § 603A.040.

189. *See id.;* David Navetta, *Nevada's Security of Personal Information Law Post Four: Encryption and PCI Compliance Requirements*, INFORMATION LAW GROUP (July 23, 2009, 7:16 PM), http://www.infolawgroup.com/2009/07/articles/nevada-security-of-personal-in/nevadas-security-of-personal-information-law-post-four-encryption-and-pci-compliance-requirements.

190. § 603A.215(5)(b).

However, the statute also requires any data collector to comply with "the current version of the Payment Card Industry ("PCI") Data Security Standard, as adopted by the PCI Security Standards Council or its successor organization[s]."[191] It is unclear whether compliance with the National Institute of Standards and Technology ("NIST") trumps the requirements under the PCI Data Security Standard. Since the PCI is considered more of a "moving target,"[192] it may be that the Nevada state legislature also incorporated the NIST standard in order to make compliance with the law easier to follow.

The most important aspect of the Nevada law concerns its safe harbor provision. Data collectors, as defined above, *shall not be liable* for damages sustained as a result of a data breach if "(a) [t]he data collector is in compliance with this section; and (b) [t]he breach is not caused by the gross negligence or intentional misconduct of the data collector, its officers, employees, or agents."[193] The law therefore insulates from monetary liability any entity that follows either the PCI or NIST standard for the encryption of personal information. Unfortunately, the law fails to provide any specific penalties for noncompliance with the law, and does not establish a private cause of action.[194] The law may be used, however, to establish the standard of care in an action for negligence and be used to prove that an entity failed to take reasonable measures under the law.[195] The Nevada statute is therefore a step in the right direction, but has certain flaws that would need to be addressed if it were to be copied at the federal level.

3. The Massachusetts Model

In January 2009, Massachusetts enacted its own law dealing with the electronic storage of personal information, which had a compliance deadline of March 1, 2010.[196] This regulation, which implements certain provisions of the Massachusetts General Laws involving security breaches,[197] is different from Nevada's in many respects. One of the differences is that the Massachusetts provision requires "every person

191. § 603A.215(1).

192. *See* Navetta, *supra* note 195. Navetta mentions that "[o]ne of the biggest problems with the PCI compliance requirement under the Security Law is that PCI is constantly being changed and updated." *Id.* He also states that the PCI standard is "ambiguous as written in many sections." *Id.*

193. § 603A.215(3).

194. *See generally* § 603A.

195. *See* David Navetta, *Nevada's Security of Personal Information Law Post Five: Remedies, Penalties and Enforcement*, INFORMATION LAW GROUP (July 24, 2009, 7:00 AM), http://www.infolawgroup.com/2009/07/articles/penalties-and-fines/nevadas-security-of-personal-information-law-post-five-remedies-penalties-and-enforcement/.

196. 201 MASS. CODE REGS. 17.05 (2008).

197. 201 MASS. CODE REGS. 17.01(1) ("This regulation implements the provisions of M.G.L. c. 93H relative to the standards to be met by persons who own or license personal information about a resident of the Commonwealth."); *see also* Security Breaches, MASS. GEN. LAWS ANN. ch. 93H (West Supp. 2011).

that owns or licenses personal information about a resident" to have a written, comprehensive security program in place to safeguard this information electronically.[198] Like Nevada, Massachusetts defines "personal information" to include Social Security numbers, driver's license numbers, and financial information.[199] Among other things, the security program must include such things as "[d]esignating one or more employees to maintain . . . the program," "[i]dentifying and assessing reasonably foreseeable internal and external risks to the security" of records, regularly monitoring the program to ensure that it is working, and conducting an annual review of the security measures in place.[200] Thus, unlike Nevada, the Massachusetts law is very specific regarding what must be done to adequately secure personal information stored electronically, and requires each entity to have a written plan of action.

The Massachusetts regulation is also specific with regard to the computer systems on which personal data is stored.[201] Massachusetts requires the "[e]ncryption of all transmitted records and files containing personal information that will travel across public networks, and encryption of all data containing personal information to be transmitted wirelessly."[202] Unlike the Nevada law, which focuses more on storage and transmission on hard drives, Massachusetts also regulates personal information stored on portable devices.[203] The regulation also mandates that all computers that store personal information have "[r]easonably up-to-date versions of system security agent software which must include malware protection and reasonably up-to-date patches and virus definitions."[204]

The biggest difference between the Massachusetts and Nevada data security laws is the standards for encryption. Whereas Nevada allows residents to follow the PCI or NIST data security standards,[205] Massachusetts specifically requires a 128-bit encryption for all personal

198. 201 MASS. CODE REGS. 17.03(1).

199. 201 MASS. CODE REGS. 17.02. "Personal information" is defined as:

> [A] Massachusetts residents' first name and last name or first initial and last name in combination with any one or more of the following data elements that relate to such resident: (a) Social Security number; (b) driver's license number or state-issued identification card number; or (c) financial account number, or credit or debit card number, with or without any required security code, access code, personal identification number or password, that would permit access to a resident's financial account.

Id.

200. 201 MASS. CODE REGS. 17.03(2)(a)–(b), (h)–(i).

201. *See generally* 201 MASS. CODE REGS. 17.04 (describing security requirements for personal information stored or transmitted electronically).

202. 201 MASS. CODE REGS. 17.04(3).

203. *See* 201 MASS. CODE REGS. 17.04(5).

204. 201 MASS. CODE REGS. 17.04(7).

205. *See* NEV. REV. STAT. ANN. § 603A.215(1), (5)(b) (LexisNexis 2010).

data.[206] The Massachusetts Office of Consumer Affairs and Business Regulation has specifically stated that password-protecting data is not enough when storing data on a computer and transmitting it wirelessly.[207] Unlike Massachusetts, the Nevada provision also does not use the word "algorithmic" under its definition of encryption.[208] This has led some people to argue that the Nevada provision only requires password protection of personal data,[209] whereas Massachusetts specifically requires the "transformation of data into a form in which meaning cannot be assigned without the use of a confidential process or key."[210]

The Massachusetts regulation, like that of Nevada, is somewhat flawed regarding the penalties for non-compliance. The relevant code provision allows for civil fines up to $50,000, but this is only with regard to the improper *disposal* of personal information.[211] The only reference to any cause of action is the section which allows the Massachusetts Attorney General to bring an action for any violations of the regulation.[212] There is nothing in the law that allows Massachusetts residents to bring a lawsuit themselves for failure to comply with the law.[213]

Some entities have also complained about the costs of implementing a written policy for the protection of personal information. The Massachusetts government itself has estimated the cost of creating such a policy for a company with ten employees to be $3,000 up front and an additional $500 per month in maintenance.[214] The Chief Privacy Officer of a major Boston-based hospital operator estimated that her company would need to spend $100,000 to comply with the new regulations.[215]

---

206. MASS. GEN. LAWS ANN. ch. 93H, § 1(a) (West Supp. 2011) (defining "encrypted" as "[the] transformation of data through the use of a 128-bit or higher algorithmic process into a form in which there is a low probability of assigning meaning without use of a confidential process or key"). *See also* 201 MASS. CODE REGS. 17.01(1) (noting that the regulation implements the provisions of Massachusetts General Law Chapter 93H).

207. *See Frequently Asked Question[s] Regarding 201[Mass. Code Regs.] 17.00*, COMMONWEALTH OF MASS. OFFICE OF CONSUMER AFFAIRS AND BUS. REGULATION (Nov. 3, 2009), *available at* http://www.mass.gov/Eoca/docs/idtheft/201CMR17faqs.pdf.

208. *Compare* MASS. GEN. LAWS ANN. ch. 93H, § 1(a) (West Supp. 2011) *with* NEV. REV. STAT. ANN. § 603A.215(5)(b) (LexisNexis 2010).

209. *See, e.g.*, Dan Blacharski, *Massachusetts Encryption Law Even Stricter than Nevada's*, THEEMAILADMIN (Oct. 24, 2008), http://www.theemailadmin.com/2008/10/massachusetts-encryption-law-even-stricter-than-nevadas/.

210. 201 MASS. CODE REGS. 17.02.

211. *See* MASS. GEN. LAWS ANN. ch. 93I, § 2(b) (West Supp. 2011).

212. MASS. GEN. LAWS ANN. ch. 93H, § 6 (West Supp. 2011).

213. *See generally* 201 MASS. CODE REGS. 17.00.

214. Ben Worthen, *New Data Privacy Laws Set for Firms*, WALL ST. J., Oct. 16, 2008, at B1, *available at* http://online.wsj.com/article/SB122411532152538495.html.

215. *Id.*

Although the Massachusetts model should be lauded for its specificity, many of its provisions are simply too burdensome to be implemented properly. At the same time, it has the same problem as Nevada with regard to the lack of penalties for noncompliance. A private person whose personal information was stolen has no specific right of action under either the Nevada or Massachusetts model. If either of these two statutes is to serve as a basis for a new national law, then this issue will need to be addressed going forward.

4. Proposed Federal Legislation

Some members of Congress have taken note of the developments in Massachusetts and Nevada, and have introduced their own legislation.[216] While these bills are certainly a positive development, none appears to have much chance of becoming law. However, it is worthwhile to note how Congress believes a new law should look, and two of these proposals are worth considering here.

Under the bill introduced by Representative Bobby Rush, the Federal Trade Commission would be required to promulgate new regulations concerning the storage and disposal of personal information within one year of the law's enactment.[217] Once these regulations are set, entities that fail to follow the FTC's requirements would be subject to civil fines of up to $11,000 per day.[218] The law would also only apply to those that meet the definition of an "information broker" and would eliminate noncommercial entities and most other types of businesses from regulation.[219] Only those companies that store and sell personal information as a business would be regulated under the bill.

The most interesting aspect of Representative Rush's proposal concerns the remedy for persons whose data has been breached. The Rush bill requires an information broker to notify the affected individuals if a security breach occurs, and provides for penalties in the event of noncompliance.[220] During the course of notification, however, the broker must provide notice that the affected individuals are

216. *See, e.g.*, *See* Data Accountability and Trust Act, H.R. 2221, 111th Cong. (2009); Data Security and Breach Notification Act, S. 3742, 111th Cong. (2010).

217. *See* H.R. 2221, 111th Cong. § 2(a). The definition of "personal information" is nearly identical to the Nevada and Massachusetts laws and concerns names, Social Security numbers, driver's license numbers, and credit card information. *See id.* § 5(7) (defining "personal information").

218. H.R. 2221, 111th Cong. § 4(c)(2)(A)(i).

219. *See* H.R. 2221, 111th Cong. § 5(6)(A):

> The term 'information broker' . . . means a commercial entity whose business is to collect, assemble, or maintain personal information concerning individuals who are not current or former customers of such entity in order to sell such information or provide access to such information to any nonaffiliated third party in exchange for consideration, whether such collection, assembly, or maintenance of personal information is performed by the information broker directly, or by contract or subcontract with any other entity.

220. *See* H.R. 2221, 111th Cong. § 4(c)(2)(A)(ii).

"entitled to receive, at no cost to the individuals, consumer credit reports on a quarterly basis for a period of 2 years."[221] Although the bill says nothing about where this cost would come from, we can presume it would be paid out of the pocket of the entity that lost the data in the first place. This alone would provide a tremendous economic incentive for companies to encrypt personal information. However, after passage in the House, the Rush bill died in the Senate.[222]

The more recent bill worth discussion was introduced by Senators Pryor and Rockefeller in August of 2010, titled the Data Security and Breach Notification Act.[223] Under this bill, the FTC would again be directed to create a system of regulations for the electronic storage of personal information.[224] In creating these regulations, the FTC would be required to consider the size, nature, scope, and complexity of the covered entities.[225] The cost of any regulation would also be a factor to consider,[226] which the Massachusetts law failed to address.[227] Standards for encryption would be adopted using technology from "an established standards setting body which renders such data indecipherable in the absence of associated cryptographic keys necessary to enable decryption of such data."[228] Enforcement of these provisions could be initiated by State Attorneys General, but the bill does not appear to provide individuals with a private right of action.[229] Instead, the State Attorneys General would be entrusted "to obtain damages, restitution, or other compensation" on behalf of the affected residents of their respective states.[230] The bill was referred to committee but was cleared at the end of the 111th Congressional Session and has not been reintroduced.[231]

IV. A NEW MODEL FOR NATIONAL REFORM

The Massachusetts, Nevada, and proposed—but failed—federal laws provide a great starting point, but all have some flaws. Forcing every entity in the county that stores personal information to create a lengthy security program seems far too costly to implement correctly.

221. H.R. 2221, 111th Cong. § 3(d)(2)(C)(i).

222. *See* H.R. 2221: Data Accountability and Trust Act, GOVTRACK.US, http://www.govtrack.us/congress/bill.xpd?bill=h111-2221 (last visited Oct. 2, 2011); *Schoolhouse Rock: How a Bill Becomes a Law*, YOUTUBE (Apr. 1, 2010), http://www.youtube.com/watch?v=mEJL2Uuv-oQ.

223. Data Security and Breach Notification Act, S. 3742, 111th Cong. (2010).

224. *Id.* § 2(a).

225. *Id.* § 2(a)(1)(A).

226. *See, e.g., id.* § 2(a)(1)(C) (taking into consideration the implementation costs of safeguarding personal information).

227. *See* Worthen, *supra* note 214.

228. S. 3742 § 5(5).

229. *See id.* § 4(c)(1).

230. *Id.* § 4(c)(1)(C).

231. *S. 3742: Data Security and Breach Notification Act of 2010*, GOVTRACK.US, http://www.govtrack.us/congress/bill.xpd?bill=s111-3742 (last visited Oct. 2, 2011).

It also seems unnecessary to require small businesses, which may keep only their employees' personal information, to have to go through the trouble of encrypting these files with 128-bit protection when a simple password on these documents would likely be enough. Mandating fines for non-compliance is a good start, but persons whose information was compromised should also be entitled to compensation and a right of recovery.

Below, the ideal provisions of a new national model for personal data protection are discussed, and an attempt is made to create a basic statute that can serve as the basis for future legislation. The proposed law would be directed at nearly every entity that stores or transmits personal information and would require such entities to protect these files using a national encryption standard. In the event that such information is compromised, the proposal would require the entity to notify all affected individuals and provide a fixed amount of monetary compensation that could be used to enroll in a credit monitoring service. Should the entity fail to follow the notification and payment provisions, individuals would be provided with a right of action to sue in federal court. Importantly, the proposal would also carve out an explicit safe harbor provision in the law; any entity that adheres to these new duties would be immune from further liability.

A. *Scope of the New Law*

Perhaps the most basic question we should start with is: *to whom should the law apply*? Mom-and-pop type establishments, which only keep a small volume of personal information, should be exempt from any requirements, although this should not necessarily absolve them of liability in the event their data is lost or stolen. It seems like any business with less than twenty-five employees would be a good cutoff for exemption under the new law. At the same time, it is clear that the law should apply to any business, nonprofit, or information broker that collects and *stores or transmits* personal information on any customer or operates a marketing business that legally provides such information to third parties. This would not include ordinary retailers who merely swipe credit cards, but it *would* apply to online companies that do business over the Internet and require a three-digit card security code for purchases. For the moment, and because it would likely have no shot at passage, we will exempt governmental organizations from compliance.

The other issue to be considered regarding the scope of the law is deciding what should be considered "personal information." Since Nevada, Massachusetts, and the proposed federal bills seem to have settled on a definition, it does not seem prudent to mess with it here. Under the new model, personal information would include a person's first name or first initial and last name, combined with either his or her Social Security number; driver's license number; or credit card,

debit card, or other financial account number. It is tempting to include email and home address within the definition, but the focus of the law should be on information that can be used for identity theft. Spamming and direct mail marketing can be left alone for the moment.

B. *Encryption Standards*

Although it is a lofty goal to mandate 128-bit encryption on any file containing personal information, such a requirement would seem overly burdensome for things such as emails and other documents that may contain personal information on a single person. In these cases, simple password protection would seem appropriate for file storage, although any transmission over the Internet or via email should require encryption technology. For databases, spreadsheets, and other files containing hundreds or even thousands of rows with this type of data, however, a minimum standard for encryption should be met for both storage and transmission.

Under the new law, the National Institute of Standards and Technology would be directed to create a uniform standard for encryption technology, which would be reviewed every twelve months. This process should not be too difficult, considering the NIST already has a list of approved advanced encryption standards.[232] The NIST would also be required to come up with a uniform standard for password protecting files that contain a minimum amount of personal information. Software developers could then use this information to create programs that password-protect files at little or no cost to the entity.

C. *Notification and Insurance Issues*

In the event of a data breach, the new law would require entities to notify all those affected and would trump all existing state notification statutes.[233] This notification would include a detailed description re-

232. *See Advanced Encryption Standard Algorithm Validation List*, NAT'L INST. OF STANDARDS AND TECH., http://csrc.nist.gov/groups/STM/cavp/documents/aes/aesval.html (last updated Oct. 2, 2011).

233. *See* ALASKA STAT. § 45.48.010 (2010); ARIZ. REV. STAT. ANN. § 44-7501 (Supp. 2010); ARK. CODE ANN. § 4-110-105 (Supp. 2011); CAL. CIV. CODE § 1798.82 (West 2009); COLO. REV. STAT. § 6-1-716 (2011); CONN. GEN. STAT. § 36a-701b (Supp. 2011); DEL. CODE ANN. tit. 6, § 12B-102 (2005); D.C. CODE § 28-3852 (Supp. 2011); FLA. STAT. § 817.5681 (2005); GA. CODE ANN. § 10-1-912 (2005); HAW. REV. STAT. ANN. § 487N-2 (LexisNexis 2009); IDAHO CODE ANN. § 28-51-105 (Supp. 2011); 815 ILL. COMP. STAT. ANN. 530/5–30 (West 2008); IND. CODE ANN. §§ 24-4.9-3-1 to -2 (West Supp. 2011); IOWA CODE ANN. §§ 715C.1–.2 (West Supp. 2011); KAN. STAT. ANN. § 50-7a02 (Supp. 2009); LA. REV. STAT. ANN. § 51:3074 (Supp. 2011); ME. REV. STAT. ANN. tit. 10, § 1348 (2009 & Supp. 2010); MD. CODE ANN., COM. LAW §§ 14-3501 to -3508 (LexisNexis Supp. 2010); MASS. GEN. LAWS ANN. ch. 93H, § 3 (West Supp. 2011); MICH. COMP. LAWS ANN. § 445.72 (West Supp. 2011); MINN. STAT. ANN. § 325E.61 (West 2011); MONT. CODE ANN. § 30-14-1704 (2009); NEB. REV. STAT. ANN. §§ 87-801 to -807 (LexisNexis 2007); NEV. REV. STAT. ANN.

garding what information has been compromised and would direct individuals on how to obtain credit monitoring. Most importantly, the notification provision would inform the affected individual that they are *automatically and immediately entitled* to a cash payout of $500. Both the notification and payment provisions would need to be fulfilled within thirty business days, which seems a reasonable time period no matter how large the organization. Instead of letting the entity decide what credit-monitoring service to use, the affected individuals should have the right to decide for themselves whether they wish to enroll in credit monitoring or take the chance that their identities might be stolen, using the $500 payment to finance the service. The current cost of credit monitoring is approximately $15 per month.[234] Two years of credit monitoring would cost an individual around $360, leaving approximately $140 left over as a small representation of the time and energy spent deciding what to do about the problem. Individuals would not have the right to opt-out of this payment and file suit to collect damages in court.

In order to finance this payout, entities that collect and store personal information on more than 100 individuals would be required to obtain data protection insurance. This would necessarily include many small businesses that store the credit card or other financial information of their customers or members. However, since the law would require these entities to encrypt and password protect personal information in the first place—and since the law would create an entirely new insurance pool of like organizations—the cost of such a requirement should be relatively low. Entities that keep personal information on fewer than 100 people would be exempt from the insurance requirement but would have the same requirements when it comes to the immediate $500 cash payout.

D. *Penalties*

The penalties for noncompliance with the law should be stiff lest any entity decide it is economically advantageous to ignore the new law. As in the Pryor and Rockefeller bill, the new national statute

§§ 603A.010–.920 (LexisNexis 2010); N.H. REV. STAT. ANN. § 359-C:19 (2009); N.J. STAT. ANN. § 56:8-163 (Supp. 2011); N.Y. GEN. BUS. LAW § 899-aa (Supp. 2011); N.C. GEN. STAT. § 75-65 (2009); N.D. CENT. CODE § 51-30-02 to -03 (2007); OKLA. STAT. ANN. tit. 74, § 3113.1 (Supp. 2010); OHIO REV. CODE ANN. § 1349.19(B)(1) (LexisNexis 2006 & Supp. 2011); OR. REV. STAT. § 646A.600–.628 (2009); 73 PA. CONS. STAT. ANN. § 2303 (West 2008); R.I. GEN. LAWS § 11-49.2-3 (Supp. 2010); S.C. CODE ANN. § 39-1-90(A) (Supp. 2010); TENN. CODE ANN. § 47-18-2107 (Supp. 2011); TEX. BUS. & COM. CODE ANN. §§ 521.051, 521.053 (West Supp. 2010); UTAH CODE ANN. § 13-44-202 (LexisNexis 2009); VT. STAT. ANN. tit. 9, § 2435 (Supp. 2010); VA. CODE ANN. § 18.2-186.6 (2008); WASH. REV. CODE § 19.255.010 (2005); W. VA. CODE § 46A-2A-102 (Supp. 2011); WIS. STAT. § 134.98 (2006); WYO. STAT. ANN. § 40-12-509 (2007).

234. *See Credit Monitoring Service Reviews*, FIGHT IDENTITY THEFT, http://www.fightidentitytheft.com/credit-monitoring.html (last visited Oct. 3, 2011).

would allow each state's attorney general to initiate an action for noncompliance and would subject offenders to civil fines of up to $10,000 per day. The attorneys general would then use these proceeds for any additional damages, restitution, or other compensation for the affected residents of their state. Any entity that fails to immediately adhere to the notification and payment provisions would also be required to pay each affected individual treble damages, equal to $3,000. Such an amount would provide a strong incentive for the entity to fulfill their obligations in a timely manner, but not to a degree that would force them into bankruptcy in the event of noncompliance. In order to accomplish this, the law would create a new civil right of action to allow the affected individuals to personally sue for noncompliance. In the event an entity has a data breach and fails to pay up within a certain amount of time, the affected individuals would have the automatic right to institute a class action lawsuit in federal court and force payment.

Perhaps most importantly, the new federal statute would have a safe harbor provision insulating entities from certain liability. As long as the NIST encryption standards are followed, any entity that loses personal information *could not be held liable* in a civil action, except in the event of gross negligence or intentional misconduct. Entities that lose personal information would still be subject to the $500 payout and could still be sued for the full $3,000 in the event they fail to pay up. However, adherence to the national encryption standards would be an affirmative defense for any additional damages resulting from the data breach, and would insulate entities from increased liability.

E. *Model Statute*

Putting all these ideas together, the proposed federal law would look something like this:

THE PERSONAL INFORMATION SECURITY ACT OF 2011

(a) Definitions
  (i) "*Personal Information*" shall mean a person's first name or first initial and last name coupled with one or more of the following data elements which relate to that person:
    (A) Social Security number;
    (B) Driver's license number or government-issued identification number;
    (C) Financial account number; or
    (D) Credit or debit card number in combination with any required personal identification number, card security code, or access code.
  (ii) "*Data Collector*" shall mean any business, nonprofit, or other entity that, for any purpose, whether automated or

otherwise, handles, collects, disseminates, or otherwise transmits and/or retains personal information.

(A) *Exception.* Any business, nonprofit, or other entity which retains the personal information of fewer than 25 persons, all of whom are employed by that same business, nonprofit, or entity, shall not be considered a data collector under this act.

(iii) "*Encryption*" or "*Encrypt*" shall mean the protection of electronic data, whether in storage or transit, using an encryption technology that has been adopted by the National Institute of Standards and Technology (hereinafter NIST). The NIST shall undertake a review of these standards at least every 12 months and, when appropriate, adopt new standards based on advances in technology. The NIST will have the sole authority to determine the manner of encryption based on:

(A) The cost of encryption;

(B) The amount of personal information stored or transmitted; and

(C) The manner in which the personal information is stored and/or transmitted.

(iv) "*Data Breach*" shall mean the unauthorized acquisition of computerized personal information that compromises the security, integrity, or confidentiality of the information, and creates a substantial risk of identity theft, fraud, or misuse against the person to whom the personal information refers.

(b) REQUIREMENTS

(i) *Generally.* Within one year of the enactment of this act, all data collectors shall encrypt personal information both in the storage and transmission of such data.

(ii) *Data Breach.* In the event of a data breach, a data collector shall be required, within a reasonable time period not to exceed 30 calendar days after discovery of the data breach, to:

(A) Provide written notification to all individuals who may have been affected by the data breach;

(B) Include a detailed description in the notification regarding the exact personal information compromised and, to the extent possible, how the personal information was compromised; and

(C) Provide a check, cash voucher, or other method of payment not less than $500 to each affected individual, with information noting that the payment may be used to enroll in a credit monitoring service. The entity may not provide information regarding any credit monitoring service with whom it retains a business relationship.

(iii) *Opt Out.* Any individual given a right to payment under this subsection is not entitled to opt-out of the provision.

(c) INSURANCE
  (i) *Registration.* All data collectors must obtain data protection insurance to cover any expenses as a result of a data breach under Section (b)(ii)(C).
  (ii) *Exemptions.* Any data collector that transmits and/or retains personal information regarding fewer than 100 individuals shall not be required to obtain data protection insurance. However, in the event of a data breach, any entity falling under this subsection must fulfill all the requirements under Section (b)(ii).

(d) PENALTIES
  (i) *Attorneys General.* In the event a data collector fails to comply with Section (b)(i), any State Attorney General may bring forth an action for noncompliance, and may demand a civil penalty of $10,000 for each day the data collector has failed to comply with Section (b)(i). The Attorneys General shall use any proceeds obtained under this subsection for any additional damages, restitution, or other compensation for the affected residents of their state.
  (ii) *Personal Right of Action.* In the event a data collector fails to comply with any of the provisions set forth in Section (b)(ii), any affected individual may bring suit in a federal court of law, and shall be entitled to recover damages not less than $3,000. Each affected individual may, but is not required, to bring forth a class action lawsuit under this subsection.
  (iii) *Safe Harbor.* Any data collector that adheres to all requirements set forth in Section (b) shall not be held liable in any civil action brought forth by any individual affected by a data breach, except in the case of gross negligence or intentional misconduct on the part of the data collector.

(e) EFFECT ON OTHER LAWS
  (i) This act shall preempt all other state and federal laws that deal with the notification and/or protection of personal information.

V. CONCLUSION

The security of personal information in the digital age is a serious problem, but it does not necessarily have to be. Massachusetts and Nevada have taken a tremendous leap forward to protect the residents of their respective states from identity theft and misuse of their personal information, but more is needed. Current case law has made it clear that individuals who choose to pursue litigation have a difficult road to recovery, with standing and proving damages being the major hurdles. A new national law is needed that creates a uniform standard for the encryption of personal information stored or transmitted electronically. This new law must provide for adequate compensation for

any individuals affected by a data breach, and ensure that such persons have access to the courts in the event of noncompliance. Implementation of such a law can be both efficient and cost-effective. By creating statutory liability for entities that fail to encrypt such data, ordinary citizens will no longer suffer from the fear that comes with the loss of their personal information, and entities all across the country can take advantage of new technology to protect this type of information from loss and misuse.